**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$server\_script\_name = preg\_replace('/\/+/', '/', str\_replace('\\', '/', $\_SERVER['SCRIPT\_NAME']));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$server\_script\_filename = preg\_replace('/\/+/', '/', str\_replace('\\', '/', $\_SERVER['SCRIPT\_FILENAME']));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$tilde\_remove = preg\_replace('/^\/\~[^\/]+(.\*)$/', '$1', $server\_script\_name);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$root = preg\_replace($pattern, '', $result['path']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$user = str\_replace(preg\_replace($pattern, '', $server\_script\_filename), '', $server\_script\_name);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$host = preg\_replace('/:[0-9]+$/', '', $host);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$host = preg\_replace("/[\<\>\'\"\\\'\\\"\%\=\(\)\/\^\\*]/", '', $host);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($g5\_path['path'].'/config.php');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace($pattern, $replace, $str);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($dbconfig\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 255 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo self::makeInputArray($posts);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 356 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$header = preg\_replace('~; secure(; HttpOnly)?$~', '', $header) . '; secure; SameSite=None';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 388 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sca = preg\_replace("/[\<\>\'\"\\\'\\\"\%\=\(\)\/\^\\*]/", "", $sca);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 397 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sfl = preg\_replace("/[\<\>\'\"\\\'\\\"\%\=\(\)\/\^\\*\s]/", "", $sfl);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 415 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sst = preg\_replace("/[\<\>\'\"\\\'\\\"\%\=\(\)\/\^\\*\s]/", "", $sst);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 467 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$bo\_table = preg\_replace('/[^a-z0-9\_]/i', '', trim($\_REQUEST['bo\_table']));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 482 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$urlencode = G5\_DOMAIN.urldecode(preg\_replace("/^".urlencode($p['path'])."/", "", $urlencode));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 488 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$gr\_id = preg\_replace('/[^a-z0-9\_]/i', '', trim($\_REQUEST['gr\_id']));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 521 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$tmp\_mb\_id = substr(preg\_replace("/[^a-zA-Z0-9\_]\*/", "", $tmp\_mb\_id), 0, 20);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 527 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\common.php

MD5 Hashing algorithm.

$key = md5($\_SERVER['SERVER\_ADDR'] . $\_SERVER['SERVER\_SOFTWARE'] . $\_SERVER['HTTP\_USER\_AGENT'] . $row['mb\_password']);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\config.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($g5\_path['path'].'/version.php');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\g4\_import\_run.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$g4\_config\_file = preg\_replace('#/config.php$#i', '', $g4\_config\_file).'/config.php';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\g4\_import\_run.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

if(preg\_replace('/[^a-z]/', '', strtolower($g4['charset'])) == 'euckr')

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 346 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\g4\_import\_run.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sql = preg\_replace($source, $target, $sql);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 382 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\g4\_import\_run.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li>'.str\_replace(G5\_TABLE\_PREFIX.'write\_', '', $create\_table).' 게시글 복사</li>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 421 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\g4\_import\_run.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li>'.$table.' table 복사</li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="hd\_h1"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_URL ?>"><img src="<?php echo G5\_IMG\_URL ?>/logo.png" alt="<?php echo $config['cf\_title']; ?>"></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="gnb\_1dli <?php echo $add\_class; ?>" style="z-index:<?php echo $gnb\_zindex--; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $row['me\_link']; ?>" target="\_<?php echo $row['me\_target']; ?>" class="gnb\_1da"><?php echo $row['me\_name'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="gnb\_2dli"><a href="<?php echo $row2['me\_link']; ?>" target="\_<?php echo $row2['me\_target']; ?>" class="gnb\_2da"><?php echo $row2['me\_name'] ?></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="gnb\_empty">메뉴 준비 중입니다.<?php if ($is\_admin) { ?> <a href="<?php echo G5\_ADMIN\_URL; ?>/menu\_list.php">관리자모드 &gt; 환경설정 &gt; 메뉴설정</a>에서 설정하실 수 있습니다.<?php } ?></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $row['me\_link']; ?>" target="\_<?php echo $row['me\_target']; ?>" class="gnb\_al\_a"><?php echo $row['me\_name'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 174 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $row2['me\_link']; ?>" target="\_<?php echo $row2['me\_target']; ?>"><?php echo $row2['me\_name'] ?></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="gnb\_empty">메뉴 준비 중입니다.<?php if ($is\_admin) { ?> <br><a href="<?php echo G5\_ADMIN\_URL; ?>/menu\_list.php">관리자모드 &gt; 환경설정 &gt; 메뉴설정</a>에서 설정하실 수 있습니다.<?php } ?></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 219 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (!defined("\_INDEX\_")) { ?><h2 id="container\_title"><span title="<?php echo get\_text($g5['title']); ?>"><?php echo get\_head\_title($g5['title']); ?></span></h2><?php }

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $config['cf\_add\_meta'].PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<title><?php echo $g5\_head\_title; ?></title>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<link rel="stylesheet" href="'.run\_replace('head\_css\_url', G5\_CSS\_URL.'/'.(G5\_IS\_MOBILE?'mobile':'default').$shop\_css.'.css?ver='.G5\_CSS\_VER, G5\_URL).'">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var g5\_is\_member = "<?php echo isset($is\_member)?$is\_member:''; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var g5\_is\_admin = "<?php echo isset($is\_admin)?$is\_admin:''; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var g5\_bo\_table = "<?php echo isset($bo\_table)?$bo\_table:''; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var g5\_sca = "<?php echo isset($sca)?$sca:''; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var g5\_editor = "<?php echo ($config['cf\_editor'] && $board['bo\_use\_dhtml\_editor'])?$config['cf\_editor']:''; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $config['cf\_add\_script'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<body<?php echo isset($g5['body\_script']) ? $g5['body\_script'] : ''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="hd\_login\_msg">'.$sr\_admin\_msg.get\_text($member['mb\_nick']).'님 로그인 중 ';

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\index.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

from `{$g5['board\_table']}` a left join `{$g5['group\_table']}` b on (a.gr\_id=b.gr\_id)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div style="float:left;<?php echo $lt\_style ?>" class="lt\_wr">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo latest('basic', $row['bo\_table'], 6, 24);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\orderupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_cart\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\orderupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_cart\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\orderupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['g5\_shop\_inicis\_log\_table']}` (

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\orderupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_cart\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\orderupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['g5\_shop\_order\_data\_table']}` (

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\orderupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_inicis\_log\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\orderupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_inicis\_log\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\orderupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_order\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\orderupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_order\_data\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\orderupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['g5\_shop\_coupon\_zone\_table']}` (

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\orderupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_coupon\_table']}`

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $config['cf\_analytics'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\tail.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == 'super') { ?><!-- <div style='float:left; text-align:center;'>RUN TIME : <?php echo get\_microtime()-$begin\_time; ?><br></div> --><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\yc4\_import.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="hd\_h1"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\yc4\_import.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_URL ?>"><img src="<?php echo G5\_IMG\_URL ?>/logo.jpg" alt="<?php echo $config['cf\_title']; ?>"></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\yc4\_import.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ((!$bo\_table || $w == 's' ) && !defined("\_INDEX\_")) { ?><div id="container\_title"><?php echo $g5['title'] ?></div><?php } ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\yc4\_import\_run.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$g4\_config\_file = preg\_replace('#/config.php$#i', '', $g4\_config\_file).'/config.php';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\yc4\_import\_run.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="hd\_h1"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\yc4\_import\_run.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_URL ?>"><img src="<?php echo G5\_IMG\_URL ?>/logo.jpg" alt="<?php echo $config['cf\_title']; ?>"></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\yc4\_import\_run.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ((!$bo\_table || $w == 's' ) && !defined("\_INDEX\_")) { ?><div id="container\_title"><?php echo $g5['title'] ?></div><?php } ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 190 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\yc4\_import\_run.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$g4[$k] = preg\_replace('/[^0-9A-Za-z\_]/', '', $v);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\yc4\_import\_run.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

if(preg\_replace('/[^a-z]/', '', strtolower($g4['charset'])) == 'euckr')

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $config['cf\_title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" id="btn\_gnb" class="btn\_gnb\_close <?php echo $adm\_menu\_cookie['btn\_gnb'];?>">메뉴</button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="logo"><a href="<?php echo correct\_goto\_url(G5\_ADMIN\_URL); ?>"><img src="<?php echo G5\_ADMIN\_URL ?>/img/logo.png" alt="<?php echo get\_text($config['cf\_title']); ?> 관리자"></a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo G5\_ADMIN\_URL ?>/member\_form.php?w=u&amp;mb\_id=<?php echo $member['mb\_id'] ?>">관리자정보</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<nav id="gnb" class="gnb\_large <?php echo $adm\_menu\_cookie['gnb']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="gnb\_li<?php echo $current\_class;?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" class="btn\_op menu-<?php echo $key; ?> menu-order-<?php echo $jj; ?>" title="<?php echo $button\_title; ?>"><?php echo $button\_title;?></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h3><?php echo $menu['menu'.$key][0][1];?></h3>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo print\_menu1('menu'.$key, 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 205 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="container" class="<?php echo $adm\_menu\_cookie['container']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 207 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="container\_title"><?php echo $g5['title'] ?></h1>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$content = file($text, false);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include($theme\_config\_file);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 360 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.lib.php

MD5 Hashing algorithm.

$token = md5(uniqid(rand(), true));

**STANDARD: Potentially Unsafe Code - fopen**

Line: 397 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.lib.php

if ( $handle = @fopen( $htaccess\_file, 'w' ) ) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 397 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if ( $handle = @fopen( $htaccess\_file, 'w' ) ) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 398 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $handle, 'Order deny,allow' . "\n" );

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 399 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $handle, 'Deny from all' . "\n" );

**STANDARD: Potentially Unsafe Code - fopen**

Line: 407 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.lib.php

if ( $handle = @fopen( $index\_file, 'w' ) ) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 407 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if ( $handle = @fopen( $index\_file, 'w' ) ) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 408 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $handle, '' );

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 417 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$txt\_files = glob($log\_path.'

**STANDARD: Potentially Unsafe Code - exec**

Line: 493 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.lib.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

ius', $value))) || preg\_match('/^(?=.\*token\()(?=.\*xmlhttprequest\()(?=.\*send\().\*$/im', $value) || (preg\_match('/[onload|onerror|focus]=.\*/ius', $value) && preg\_match('/(eval|expression|exec|prompt)(\s\*)\((.\*)\)/ius', $value)) ){

**STANDARD: Potentially Unsafe Code - eval**

Line: 493 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.lib.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

ius', $value))) || preg\_match('/^(?=.\*token\()(?=.\*xmlhttprequest\()(?=.\*send\().\*$/im', $value) || (preg\_match('/[onload|onerror|focus]=.\*/ius', $value) && preg\_match('/(eval|expression|exec|prompt)(\s\*)\((.\*)\)/ius', $value)) ){

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 493 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.lib.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

ius', $value))) || preg\_match('/^(?=.\*token\()(?=.\*xmlhttprequest\()(?=.\*send\().\*$/im', $value) || (preg\_match('/[onload|onerror|focus]=.\*/ius', $value) && preg\_match('/(eval|expression|exec|prompt)(\s\*)\((.\*)\)/ius', $value)) ){

**MEDIUM: Potentially Unsafe Code - md5**

Line: 555 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.lib.php

MD5 Hashing algorithm.

$admin\_key = md5($member['mb\_datetime'] . get\_real\_client\_ip() . $\_SERVER['HTTP\_USER\_AGENT']);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 588 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($file);

**STANDARD: Potentially Unsafe Code - phpinfo**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.menu100.php

This debugging function can expose sensitive data to an attacker. Perform a manual check to ensure that its out put data is not visible to normal users.

array('100500', 'phpinfo()', G5\_ADMIN\_URL.'/phpinfo.php', 'cf\_phpinfo')

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

Copyright &copy; <?php echo $\_SERVER['HTTP\_HOST']; ?>. All rights reserved. <?php echo $print\_version; ?><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\admin.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <p>실행시간 : <?php echo get\_microtime() - $begin\_time; ?> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">설정된 관리권한</span><span class="ov\_num"><?php echo number\_format($total\_count) ?>건</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx ?>" id="stx" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="au\_menu[<?php echo $i ?>]" value="<?php echo $row['au\_menu'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id[<?php echo $i ?>]" value="<?php echo $row['mb\_id'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i; ?>" class="sound\_only"><?php echo $row['mb\_nick'] ?>님 권한</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk[]" value="<?php echo $i ?>" id="chk\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbid"><a href="?sfl=a.mb\_id&amp;stx=<?php echo $row['mb\_id'] ?>"><?php echo $row['mb\_id'] ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_auth\_mbnick"><?php echo $mb\_nick ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $row['au\_menu'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $auth\_menu[$row['au\_menu']] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_auth"><?php echo $row['au\_auth'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 160 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $pagelist;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 192 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_id" value="<?php echo $mb\_id ?>" id="mb\_id" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 204 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<option value="'.$key.'">'.$key.' '.$value.'</option>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 228 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $captcha\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 246 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_js;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list\_delete.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$mb\_id = isset($\_POST['mb\_id'][$k]) ? preg\_replace('/[^a-zA-Z0-9\_]/', '', $\_POST['mb\_id'][$k]) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_list\_delete.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$au\_menu = isset($\_POST['au\_menu'][$k]) ? preg\_replace('/[^a-zA-Z0-9\_]/', '', $\_POST['au\_menu'][$k]) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$au\_menu = isset($\_POST['au\_menu']) ? preg\_replace('/[^0-9a-z\_]/i', '', $\_POST['au\_menu']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$post\_r = isset($\_POST['r']) ? preg\_replace('/[^0-9a-z\_]/i', '', $\_POST['r']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$post\_w = isset($\_POST['w']) ? preg\_replace('/[^0-9a-z\_]/i', '', $\_POST['w']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$post\_d = isset($\_POST['d']) ? preg\_replace('/[^0-9a-z\_]/i', '', $\_POST['d']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\auth\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$site\_url = preg\_replace('/^www\./', '', strtolower($\_SERVER['SERVER\_NAME']));

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $mb['mb\_id'] ?>" id="mb\_id">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt"> 아이디</span><span class="ov\_num"><?php echo $mb['mb\_id'] ?></span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt"> 이름</span><span class="ov\_num"><?php echo get\_text($mb['mb\_name']); ?></span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt"> 닉네임</span><span class="ov\_num"><?php echo $mb['mb\_nick'] ?></span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<option value=\"".$row['gr\_id']."\">".$row['gr\_subject']."</option>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>" id="sst">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>" id="sod">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>" id="sfl">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>" id="stx">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>" id="page">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $mb['mb\_id'] ?>" id="mb\_id">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i; ?>" class="sound\_only"><?php echo $row['gr\_subject'] ?> 그룹</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk[]" value="<?php echo $row['gm\_id'] ?>" id="chk\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_grid"><a href="<?php echo G5\_BBS\_URL; ?>/group.php?gr\_id=<?php echo $row['gr\_id'] ?>"><?php echo $row['gr\_id'] ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_category"><?php echo $row['gr\_subject'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo $row['gm\_datetime'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">접근가능한 그룹이 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="gr\_id" value="<?php echo $gr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.mb\_id"<?php echo get\_selected($sfl, "a.mb\_id") ?>>회원아이디</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx ?>" id="stx" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo $token ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="gr\_id" value="<?php echo $gr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><?php echo subject\_sort\_link('b.mb\_id', 'gr\_id='.$gr\_id) ?>회원아이디</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><?php echo subject\_sort\_link('b.mb\_name', 'gr\_id='.$gr\_id) ?>이름</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><?php echo subject\_sort\_link('b.mb\_nick', 'gr\_id='.$gr\_id) ?>별명</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><?php echo subject\_sort\_link('b.mb\_today\_login', 'gr\_id='.$gr\_id) ?>최종접속</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><?php echo subject\_sort\_link('a.gm\_datetime', 'gr\_id='.$gr\_id) ?>처리일시</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i; ?>" class="sound\_only"><?php echo $row['mb\_nick'] ?> 회원</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk[]" value="<?php echo $row['gm\_id'] ?>" id="chk\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_grid"><?php echo $group ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbid"><?php echo $row['mb\_id'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbname"><?php echo get\_text($row['mb\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_name sv\_use"><?php echo $mb\_nick ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo substr($row['mb\_today\_login'],2,8) ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo $row['gm\_datetime'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroupmember\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;gr\_id=$gr\_id&page="); ?>

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['group\_table']}` ADD `gr\_device` ENUM('both','pc','mobile') NOT NULL DEFAULT 'both' AFTER `gr\_subject` ", false);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><label for="gr\_id">그룹 ID<?php echo $sound\_only ?></label></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="gr\_id" value="<?php echo $group['gr\_id'] ?>" id="gr\_id" <?php echo $gr\_id\_attr; ?> class="<?php echo $gr\_id\_attr; ?> alnum\_ frm\_input" maxlength="10">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="'.G5\_BBS\_URL.'/group.php?gr\_id='.$group['gr\_id'].'" class="btn\_frmline">게시판그룹 바로가기</a>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="gr\_subject" value="<?php echo get\_text($group['gr\_subject']) ?>" id="gr\_subject" required class="required frm\_input" size="80">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="./board\_form.php?gr\_id='.$gr\_id.'" class="btn\_frmline">게시판생성</a>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="both"<?php echo get\_selected($group['gr\_device'], 'both', true); ?>>PC와 모바일에서 모두 사용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="pc"<?php echo get\_selected($group['gr\_device'], 'pc'); ?>>PC 전용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mobile"<?php echo get\_selected($group['gr\_device'], 'mobile'); ?>>모바일 전용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="text" id="gr\_admin" name="gr\_admin" class="frm\_input" value="'.$gr['gr\_admin'].'" maxlength="20">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="hidden" id="gr\_admin" name="gr\_admin" value="'.$gr['gr\_admin'].'">'.$gr['gr\_admin'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="gr\_use\_access" value="1" id="gr\_use\_access" <?php echo $gr['gr\_use\_access']?'checked':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="./boardgroupmember\_list.php?gr\_id='.$gr\_id.'">'.$row1['cnt'].'</a>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row">여분필드<?php echo $i ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="gr\_<?php echo $i ?>\_subj">여분필드 <?php echo $i ?> 제목</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="gr\_<?php echo $i ?>\_subj" value="<?php echo isset($group['gr\_'.$i.'\_subj']) ? get\_text($group['gr\_'.$i.'\_subj']) : ''; ?>" id="gr\_<?php echo $i ?>\_subj" class="frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="gr\_<?php echo $i ?>">여분필드 <?php echo $i ?> 내용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./boardgroup\_list.php?<?php echo $qstr ?>" class="btn btn\_02">목록</a>

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['group\_table']}` ADD `gr\_device` ENUM( 'both', 'pc', 'mobile' ) NOT NULL DEFAULT 'both' AFTER `gr\_subject` ", false);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">전체그룹</span><span class="ov\_num"> <?php echo number\_format($total\_count) ?>개</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="gr\_subject"<?php echo get\_selected($sfl, "gr\_subject"); ?>>제목</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="gr\_id"<?php echo get\_selected($sfl, "gr\_id"); ?>>ID</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="gr\_admin"<?php echo get\_selected($sfl, "gr\_admin"); ?>>그룹관리자</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" id="stx" value="<?php echo $stx ?>" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="group\_id[<?php echo $i ?>]" value="<?php echo $row['gr\_id'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i; ?>" class="sound\_only"><?php echo get\_text($row['gr\_subject']); ?> 그룹</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk[]" value="<?php echo $i ?>" id="chk\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><a href="<?php echo G5\_BBS\_URL ?>/group.php?gr\_id=<?php echo $row['gr\_id'] ?>"><?php echo $row['gr\_id'] ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="gr\_subject\_<?php echo $i; ?>" class="sound\_only">그룹제목</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="gr\_subject[<?php echo $i ?>]" value="<?php echo get\_text($row['gr\_subject']) ?>" id="gr\_subject\_<?php echo $i ?>" class="tbl\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="gr\_admin\_<?php echo $i; ?>" class="sound\_only">그룹관리자</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><a href="./board\_list.php?sfl=a.gr\_id&amp;stx=<?php echo $row['gr\_id'] ?>"><?php echo $row2['cnt'] ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="gr\_use\_access\_<?php echo $i; ?>" class="sound\_only">접근회원 사용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="gr\_use\_access[<?php echo $i ?>]" <?php echo $row['gr\_use\_access']?'checked':'' ?> value="1" id="gr\_use\_access\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><a href="./boardgroupmember\_list.php?gr\_id=<?php echo $row['gr\_id'] ?>"><?php echo $row1['cnt'] ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="gr\_order\_<?php echo $i; ?>" class="sound\_only">메인메뉴 출력순서</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="gr\_order[<?php echo $i ?>]" value="<?php echo $row['gr\_order'] ?>" id="gr\_order\_<?php echo $i ?>" class="tbl\_input" size="2">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="gr\_device\_<?php echo $i; ?>" class="sound\_only">접속기기</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="gr\_device[<?php echo $i ?>]" id="gr\_device\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="both"<?php echo get\_selected($row['gr\_device'], 'both'); ?>>모두</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="pc"<?php echo get\_selected($row['gr\_device'], 'pc'); ?>>PC</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mobile"<?php echo get\_selected($row['gr\_device'], 'mobile'); ?>>모바일</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mng td\_mng\_s"><?php echo $s\_upd ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $pagelist;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\boardgroup\_list\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$gr\_id = preg\_replace('/[^a-z0-9\_]/i', '', $post\_group\_id[$k]);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_copy.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title']; ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_copy.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>" id="bo\_table">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_copy.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_copy.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $bo\_table ?></td>

**STANDARD: Potentially Unsafe Code - fopen**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_copy\_update.php

$f = @fopen($file, 'w');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_copy\_update.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$f = @fopen($file, 'w');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_copy\_update.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($f, '');

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['board\_table']}` ADD `bo\_device` ENUM( 'both', 'pc', 'mobile' ) NOT NULL DEFAULT 'both' AFTER `bo\_subject` ", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['board\_table']}` ADD `bo\_mobile\_skin` VARCHAR(255) NOT NULL DEFAULT '' AFTER `bo\_skin` ", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['board\_table']}` ADD `bo\_gallery\_width` INT NOT NULL AFTER `bo\_gallery\_cols`, ADD `bo\_gallery\_height` INT NOT NULL DEFAULT '0' AFTER `bo\_gallery\_width`, ADD `bo\_mobile\_gallery\_width` INT NOT NULL DEFAULT '0' AFTER `bo\_gallery\_height`, ADD `bo\_mobile\_gallery\_height` INT NOT NULL DEFAULT '0' AFTER `bo\_mobile\_gallery\_width` ", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['board\_table']}` ADD `bo\_mobile\_subject\_len` INT(11) NOT NULL DEFAULT '0' AFTER `bo\_subject\_len` ", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['board\_table']}` ADD `bo\_mobile\_page\_rows` INT(11) NOT NULL DEFAULT '0' AFTER `bo\_page\_rows` ", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['board\_table']}` ADD `bo\_mobile\_content\_head` TEXT NOT NULL AFTER `bo\_content\_head`, ADD `bo\_mobile\_content\_tail` TEXT NOT NULL AFTER `bo\_content\_tail`", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['board\_table']}` ADD `bo\_use\_cert` ENUM('','cert','adult') NOT NULL DEFAULT '' AFTER `bo\_use\_email` ", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['board\_table']}` ADD `bo\_use\_sns` TINYINT NOT NULL DEFAULT '0' AFTER `bo\_use\_cert` ", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$result = sql\_query(" select bo\_table from `{$g5['board\_table']}` ");

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['write\_prefix']}{$row['bo\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " SHOW COLUMNS FROM `{$g5['board\_table']}` LIKE 'bo\_use\_cert' ";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['board\_table']}` CHANGE `bo\_use\_cert` `bo\_use\_cert` ENUM('','cert','adult','hp-cert','hp-adult') NOT NULL DEFAULT '' ", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['board\_table']}` ADD `bo\_use\_list\_file` TINYINT NOT NULL DEFAULT '0' AFTER `bo\_use\_list\_view` ", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$result = sql\_query(" select bo\_table from `{$g5['board\_table']}` ");

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['write\_prefix']}{$row['bo\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['board\_table']}` ADD `bo\_mobile\_subject` VARCHAR(255) NOT NULL DEFAULT '' AFTER `bo\_subject` ", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['board\_table']}` ADD `bo\_use\_captcha` TINYINT NOT NULL DEFAULT '0' AFTER `bo\_use\_sns` ", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['board\_table']}` ADD `bo\_select\_editor` VARCHAR(50) NOT NULL DEFAULT '' AFTER `bo\_use\_dhtml\_editor` ", false);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 219 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 220 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 221 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 222 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 223 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 224 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 229 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 241 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><label for="bo\_table">TABLE<?php echo $sound\_only ?></label></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 243 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_table" value="<?php echo $board['bo\_table'] ?>" id="bo\_table" <?php echo $required ?> <?php echo $readonly ?> class="frm\_input <?php echo $readonly ?> <?php echo $required ?> <?php echo $required\_valid ?>" maxlength="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 247 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($board['bo\_table']) ?>" class="btn\_frmline">게시판 바로가기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 248 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./board\_list.php?<?php echo $qstr;?>" class="btn\_frmline">목록으로</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 255 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_group\_select('gr\_id', $board['gr\_id'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 262 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_subject" value="<?php echo get\_text($board['bo\_subject']) ?>" id="bo\_subject" required class="required frm\_input" size="80" maxlength="120">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 269 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_mobile\_subject" value="<?php echo get\_text($board['bo\_mobile\_subject']) ?>" id="bo\_mobile\_subject" class="frm\_input" size="80" maxlength="120">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 277 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="both"<?php echo get\_selected($board['bo\_device'], 'both'); ?>>PC와 모바일에서 모두 사용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 278 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="pc"<?php echo get\_selected($board['bo\_device'], 'pc'); ?>>PC 전용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 279 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mobile"<?php echo get\_selected($board['bo\_device'], 'mobile'); ?>>모바일 전용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 293 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_category\_list" value="<?php echo get\_text($board['bo\_category\_list']) ?>" id="bo\_category\_list" class="frm\_input" size="70">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 294 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_category" value="1" id="bo\_use\_category" <?php echo $board['bo\_use\_category']?'checked':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 308 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo help('현재 원글수 : '.number\_format($board['bo\_count\_write']).', 현재 댓글수 : '.number\_format($board['bo\_count\_comment'])."\n".'게시판 목록에서 글의 번호가 맞지 않을 경우에 체크하십시오.') ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 322 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 336 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_admin" value="<?php echo $board['bo\_admin'] ?>" id="bo\_admin" class="frm\_input" maxlength="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 349 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_level\_select('bo\_list\_level', 1, 10, $board['bo\_list\_level']) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 361 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_level\_select('bo\_read\_level', 1, 10, $board['bo\_read\_level']) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 373 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_level\_select('bo\_write\_level', 1, 10, $board['bo\_write\_level']) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 385 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_level\_select('bo\_reply\_level', 1, 10, $board['bo\_reply\_level']) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 397 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_level\_select('bo\_comment\_level', 1, 10, $board['bo\_comment\_level']) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 409 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_level\_select('bo\_link\_level', 1, 10, $board['bo\_link\_level']) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 421 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_level\_select('bo\_upload\_level', 1, 10, $board['bo\_upload\_level']) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 433 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_level\_select('bo\_download\_level', 1, 10, $board['bo\_download\_level']) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 445 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_level\_select('bo\_html\_level', 1, 10, $board['bo\_html\_level']) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 463 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 478 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

댓글 <input type="text" name="bo\_count\_modify" value="<?php echo $board['bo\_count\_modify'] ?>" id="bo\_count\_modify" required class="required numeric frm\_input" size="3">개 이상 달리면 수정불가

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 490 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

댓글 <input type="text" name="bo\_count\_delete" value="<?php echo $board['bo\_count\_delete'] ?>" id="bo\_count\_delete" required class="required numeric frm\_input" size="3">개 이상 달리면 삭제불가

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 502 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_sideview" value="1" id="bo\_use\_sideview" <?php echo $board['bo\_use\_sideview']?'checked':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 517 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo option\_selected(0, $board['bo\_use\_secret'], "사용하지 않음"); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 518 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo option\_selected(1, $board['bo\_use\_secret'], "체크박스"); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 519 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo option\_selected(2, $board['bo\_use\_secret'], "무조건"); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 533 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_dhtml\_editor" value="1" <?php echo $board['bo\_use\_dhtml\_editor']?'checked':''; ?> id="bo\_use\_dhtml\_editor">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 551 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo "<option value=\"\">기본환경설정의 에디터 사용</option>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 552 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<option value=\"".$arr[$i]."\"".get\_selected($board['bo\_select\_editor'], $arr[$i]).">".$arr[$i]."</option>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 568 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_rss\_view" value="1" <?php echo $board['bo\_use\_rss\_view']?'checked':''; ?> id="bo\_use\_rss\_view">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 581 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_good" value="1" <?php echo $board['bo\_use\_good']?'checked':''; ?> id="bo\_use\_good">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 594 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_nogood" value="1" id="bo\_use\_nogood" <?php echo $board['bo\_use\_nogood']?'checked':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 607 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_name" value="1" id="bo\_use\_name" <?php echo $board['bo\_use\_name']?'checked':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 621 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_signature" value="1" id="bo\_use\_signature" <?php echo $board['bo\_use\_signature']?'checked':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 634 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_ip\_view" value="1" id="bo\_use\_ip\_view" <?php echo $board['bo\_use\_ip\_view']?'checked':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 648 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_list\_content" value="1" id="bo\_use\_list\_content" <?php echo $board['bo\_use\_list\_content']?'checked':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 662 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_list\_file" value="1" id="bo\_use\_list\_file" <?php echo $board['bo\_use\_list\_file']?'checked':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 675 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_list\_view" value="1" id="bo\_use\_list\_view" <?php echo $board['bo\_use\_list\_view']?'checked':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 688 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_email" value="1" id="bo\_use\_email" <?php echo $board['bo\_use\_email']?'checked':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 704 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo option\_selected("", $board['bo\_use\_cert'], "사용안함");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 706 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo option\_selected("cert", $board['bo\_use\_cert'], "본인확인된 회원전체");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 707 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo option\_selected("adult", $board['bo\_use\_cert'], "본인확인된 성인회원만");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 723 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_upload\_count" value="<?php echo $board['bo\_upload\_count'] ?>" id="bo\_upload\_count" required class="required numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 736 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

업로드 파일 한개당 <input type="text" name="bo\_upload\_size" value="<?php echo $board['bo\_upload\_size'] ?>" id="bo\_upload\_size" required class="required numeric frm\_input" size="10"> bytes 이하

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 748 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_file\_content" value="1" id="bo\_use\_file\_content" <?php echo $board['bo\_use\_file\_content']?'checked':''; ?>>사용

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 761 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_write\_min" value="<?php echo $board['bo\_write\_min'] ?>" id="bo\_write\_min" class="numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 774 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_write\_max" value="<?php echo $board['bo\_write\_max'] ?>" id="bo\_write\_max" class="numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 787 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_comment\_min" value="<?php echo $board['bo\_comment\_min'] ?>" id="bo\_comment\_min" class="numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 800 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_comment\_max" value="<?php echo $board['bo\_comment\_max'] ?>" id="bo\_comment\_max" class="numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 813 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_sns" value="1" id="bo\_use\_sns" <?php echo $board['bo\_use\_sns']?'checked':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 826 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_search" value="1" id="bo\_use\_search" <?php echo $board['bo\_use\_search']?'checked':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 840 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_order" value="<?php echo $board['bo\_order'] ?>" id="bo\_order" class="frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 853 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_captcha" value="1" <?php echo $board['bo\_use\_captcha']?'checked':''; ?> id="bo\_use\_captcha">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 871 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 885 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_skin\_select('board', 'bo\_skin', 'bo\_skin', $board['bo\_skin'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 897 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_mobile\_skin\_select('board', 'bo\_mobile\_skin', 'bo\_mobile\_skin', $board['bo\_mobile\_skin'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 910 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_include\_head" value="<?php echo $board['bo\_include\_head'] ?>" id="bo\_include\_head" class="frm\_input" size="50">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 922 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_include\_tail" value="<?php echo $board['bo\_include\_tail'] ?>" id="bo\_include\_tail" class="frm\_input" size="50">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 940 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $captcha\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 950 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo editor\_html("bo\_content\_head", get\_text(html\_purifier($board['bo\_content\_head']), 0)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 962 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo editor\_html("bo\_content\_tail", get\_text(html\_purifier($board['bo\_content\_tail']), 0)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 974 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo editor\_html("bo\_mobile\_content\_head", get\_text(html\_purifier($board['bo\_mobile\_content\_head']), 0)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 986 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo editor\_html("bo\_mobile\_content\_tail", get\_text(html\_purifier($board['bo\_mobile\_content\_tail']), 0)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 999 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea id="bo\_insert\_content" name="bo\_insert\_content" rows="5"><?php echo html\_purifier($board['bo\_insert\_content']); ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1012 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_subject\_len" value="<?php echo $board['bo\_subject\_len'] ?>" id="bo\_subject\_len" required class="required numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1025 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_mobile\_subject\_len" value="<?php echo $board['bo\_mobile\_subject\_len'] ?>" id="bo\_mobile\_subject\_len" required class="required numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1037 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_page\_rows" value="<?php echo $board['bo\_page\_rows'] ?>" id="bo\_page\_rows" required class="required numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1049 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_mobile\_page\_rows" value="<?php echo $board['bo\_mobile\_page\_rows'] ?>" id="bo\_mobile\_page\_rows" required class="required numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1062 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_gallery\_cols" value="<?php echo $board['bo\_gallery\_cols'] ?>" id="bo\_gallery\_cols" required class="required numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1075 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_gallery\_width" value="<?php echo $board['bo\_gallery\_width'] ?>" id="bo\_gallery\_width" required class="required numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1088 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_gallery\_height" value="<?php echo $board['bo\_gallery\_height'] ?>" id="bo\_gallery\_height" required class="required numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_mobile\_gallery\_width" value="<?php echo $board['bo\_mobile\_gallery\_width'] ?>" id="bo\_mobile\_gallery\_width" required class="required numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_mobile\_gallery\_height" value="<?php echo $board['bo\_mobile\_gallery\_height'] ?>" id="bo\_mobile\_gallery\_height" required class="required numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_table\_width" value="<?php echo $board['bo\_table\_width'] ?>" id="bo\_table\_width" required class="required numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_image\_width" value="<?php echo $board['bo\_image\_width'] ?>" id="bo\_image\_width" required class="required numeric frm\_input" size="4"> 픽셀

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_new" value="<?php echo $board['bo\_new'] ?>" id="bo\_new" required class="required numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_hot" value="<?php echo $board['bo\_hot'] ?>" id="bo\_hot" required class="required numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"<?php echo get\_selected($board['bo\_reply\_order'], 1, true); ?>>나중에 쓴 답변 아래로 달기 (기본)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0"<?php echo get\_selected($board['bo\_reply\_order'], 0); ?>>나중에 쓴 답변 위로 달기

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1210 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<option value="'.$option\_value.'" '.$selected.' >'.$order\_by\_str.' : '.$v[1].'</option>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1230 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1251 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_read\_point" value="<?php echo $board['bo\_read\_point'] ?>" id="bo\_read\_point" required class="required frm\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1263 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_write\_point" value="<?php echo $board['bo\_write\_point'] ?>" id="bo\_write\_point" required class="required frm\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1275 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_comment\_point" value="<?php echo $board['bo\_comment\_point'] ?>" id="bo\_comment\_point" required class="required frm\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1287 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_download\_point" value="<?php echo $board['bo\_download\_point'] ?>" id="bo\_download\_point" required class="required frm\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1303 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1316 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row">여분필드<?php echo $i ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1318 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bo\_<?php echo $i ?>\_subj">여분필드 <?php echo $i ?> 제목</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1319 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_<?php echo $i ?>\_subj" id="bo\_<?php echo $i ?>\_subj" value="<?php echo get\_text($board['bo\_'.$i.'\_subj']) ?>" class="frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1320 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bo\_<?php echo $i ?>">여분필드 <?php echo $i ?> 값</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1321 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_<?php echo $i ?>" value="<?php echo get\_text($board['bo\_'.$i]) ?>" id="bo\_<?php echo $i ?>" class="frm\_input extra-value-input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1324 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_grp\_<?php echo $i ?>" value="1" id="chk\_grp\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1325 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_grp\_<?php echo $i ?>">그룹적용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1326 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_all\_<?php echo $i ?>" value="1" id="chk\_all\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1327 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_all\_<?php echo $i ?>">전체적용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1339 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./board\_copy.php?bo\_table=<?php echo $board['bo\_table']; ?>" id="board\_copy" target="win\_board\_copy" class=" btn\_02 btn">게시판복사</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1340 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($board['bo\_table']); ?>" class=" btn\_02 btn">게시판 바로가기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1341 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./board\_thumbnail\_delete.php?bo\_table=<?php echo $board['bo\_table'].'&amp;'.$qstr;?>" onclick="return delete\_confirm2('게시판 썸네일 파일을 삭제하시겠습니까?');" class="btn\_02 btn">게시판 썸네일 삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1393 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

f.bo\_read\_point.value = "<?php echo $config['cf\_read\_point'] ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1394 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

f.bo\_write\_point.value = "<?php echo $config['cf\_write\_point'] ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1395 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

f.bo\_comment\_point.value = "<?php echo $config['cf\_comment\_point'] ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1396 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

f.bo\_download\_point.value = "<?php echo $config['cf\_download\_point'] ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1421 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var bo\_include\_head = "<?php echo $board['bo\_include\_head']; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1422 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var bo\_include\_tail = "<?php echo $board['bo\_include\_tail']; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1484 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo isset($captcha\_js) ? $captcha\_js : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$gr\_id = isset($\_POST['gr\_id']) ? preg\_replace('/[^a-z0-9\_]/i', '', $\_POST['gr\_id']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$bo\_admin = isset($\_POST['bo\_admin']) ? preg\_replace('/[^a-z0-9\_\, \|\#]/i', '', $\_POST['bo\_admin']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$bo\_include\_head = isset($\_POST['bo\_include\_head']) ? preg\_replace(array("#[\\\]+$#", "#(<\?php|<\?)#i"), "", substr($\_POST['bo\_include\_head'], 0, 255)) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$bo\_include\_tail = isset($\_POST['bo\_include\_tail']) ? preg\_replace(array("#[\\\]+$#", "#(<\?php|<\?)#i"), "", substr($\_POST['bo\_include\_tail'], 0, 255)) : '';

**STANDARD: Potentially Unsafe Code - fopen**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form\_update.php

if( $f = @fopen($file, 'w') ){

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form\_update.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if( $f = @fopen($file, 'w') ){

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form\_update.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($f, '');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str\_bo\_category\_list = preg\_replace("/[\<\>\'\"\\\'\\\"\%\=\(\)\/\^\\*]/", "", $bo\_category\_list);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$bo\_use\_cert = isset($\_POST['bo\_use\_cert']) ? preg\_replace('/[^0-9a-z\_]/i', '', $\_POST['bo\_use\_cert']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 286 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_form\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sql = preg\_replace($source, $target, $sql);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">생성된 게시판수</span><span class="ov\_num"> <?php echo number\_format($total\_count) ?>개</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="bo\_table"<?php echo get\_selected($sfl, "bo\_table", true); ?>>TABLE</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="bo\_subject"<?php echo get\_selected($sfl, "bo\_subject"); ?>>제목</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.gr\_id"<?php echo get\_selected($sfl, "a.gr\_id"); ?>>그룹ID</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx ?>" id="stx" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo isset($token) ? $token : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i; ?>" class="sound\_only"><?php echo get\_text($row['bo\_subject']) ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk[]" value="<?php echo $i ?>" id="chk\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_group\_select("gr\_id[$i]", $row['gr\_id']) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="gr\_id[<?php echo $i ?>]" value="<?php echo $row['gr\_id'] ?>"><?php echo $row['gr\_subject'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="board\_table[<?php echo $i ?>]" value="<?php echo $row['bo\_table'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($row['bo\_table']) ?>"><?php echo $row['bo\_table'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bo\_skin\_<?php echo $i; ?>" class="sound\_only">스킨</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_skin\_select('board', 'bo\_skin\_'.$i, "bo\_skin[$i]", $row['bo\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bo\_mobile\_skin\_<?php echo $i; ?>" class="sound\_only">모바일 스킨</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_mobile\_skin\_select('board', 'bo\_mobile\_skin\_'.$i, "bo\_mobile\_skin[$i]", $row['bo\_mobile\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bo\_subject\_<?php echo $i; ?>" class="sound\_only">게시판 제목<strong class="sound\_only"> 필수</strong></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_subject[<?php echo $i ?>]" value="<?php echo get\_text($row['bo\_subject']) ?>" id="bo\_subject\_<?php echo $i ?>" required class="required tbl\_input bo\_subject full\_input" size="10">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bo\_read\_point\_<?php echo $i; ?>" class="sound\_only">읽기 포인트</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_read\_point[<?php echo $i ?>]" value="<?php echo $row['bo\_read\_point'] ?>" id="bo\_read\_point\_<?php echo $i; ?>" class="tbl\_input" size="2">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bo\_write\_point\_<?php echo $i; ?>" class="sound\_only">쓰기 포인트</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_write\_point[<?php echo $i ?>]" value="<?php echo $row['bo\_write\_point'] ?>" id="bo\_write\_point\_<?php echo $i; ?>" class="tbl\_input" size="2">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bo\_comment\_point\_<?php echo $i; ?>" class="sound\_only">댓글 포인트</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_comment\_point[<?php echo $i ?>]" value="<?php echo $row['bo\_comment\_point'] ?>" id="bo\_comment\_point\_<?php echo $i; ?>" class="tbl\_input" size="2">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bo\_download\_point\_<?php echo $i; ?>" class="sound\_only">다운<br>포인트</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_download\_point[<?php echo $i ?>]" value="<?php echo $row['bo\_download\_point'] ?>" id="bo\_download\_point\_<?php echo $i; ?>" class="tbl\_input" size="2">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bo\_use\_sns\_<?php echo $i; ?>" class="sound\_only">SNS<br>사용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_sns[<?php echo $i ?>]" value="1" id="bo\_use\_sns\_<?php echo $i ?>" <?php echo $row['bo\_use\_sns']?"checked":"" ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 169 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bo\_use\_search\_<?php echo $i; ?>" class="sound\_only">검색<br>사용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bo\_use\_search[<?php echo $i ?>]" value="1" id="bo\_use\_search\_<?php echo $i ?>" <?php echo $row['bo\_use\_search']?"checked":"" ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bo\_order\_<?php echo $i; ?>" class="sound\_only">출력<br>순서</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 174 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bo\_order[<?php echo $i ?>]" value="<?php echo $row['bo\_order'] ?>" id="bo\_order\_<?php echo $i ?>" class="tbl\_input" size="2">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bo\_device\_<?php echo $i; ?>" class="sound\_only">접속기기</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="bo\_device[<?php echo $i ?>]" id="bo\_device\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="both"<?php echo get\_selected($row['bo\_device'], 'both', true); ?>>모두</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="pc"<?php echo get\_selected($row['bo\_device'], 'pc'); ?>>PC</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 181 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mobile"<?php echo get\_selected($row['bo\_device'], 'mobile'); ?>>모바일</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 185 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $one\_update ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 186 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $one\_copy ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 192 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 210 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, $\_SERVER['SCRIPT\_NAME'].'?'.$qstr.'&amp;page='); ?>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_thumbnail\_delete.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$files = glob($dir.'/thumb-\*');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_thumbnail\_delete.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li>'.$thumbnail.'</li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_thumbnail\_delete.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="local\_desc01 local\_desc"><p><strong>썸네일 '.$cnt.'건의 삭제 완료됐습니다.</strong></p></div>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\board\_thumbnail\_delete.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="btn\_confirm01 btn\_confirm"><a href="./board\_form.php?w=u&amp;bo\_table=<?php echo $bo\_table; ?>&amp;<?php echo $qstr; ?>">게시판 수정으로 돌아가기</a></div>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\browscap\_convert.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$rows = isset($\_GET['rows']) ? preg\_replace('#[^0-9]#', '', $\_GET['rows']) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\browscap\_convert.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

data: { rows: "<?php echo $rows; ?>" },

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\browscap\_converter.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$rows = preg\_replace('#[^0-9]#', '', $\_GET['rows']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\browscap\_converter.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<p>총 '.number\_format($total\_count).'건 중 '.number\_format($cnt).'건 변환완료<br><br>접속로그를 추가로 변환하시려면 아래 업데이트 버튼을 클릭해 주세요.</p><button type="button" id="run\_update">업데이트</button>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\cache\_file\_delete.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li>'.$cache\_file.'</li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\cache\_file\_delete.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="local\_desc01 local\_desc"><p><strong>최신글 캐시파일 '.$cnt.'건 삭제 완료됐습니다.</strong><br>프로그램의 실행을 끝마치셔도 좋습니다.</p></div>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\captcha\_file\_delete.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li>'.$gcaptcha\_file.'</li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\captcha\_file\_delete.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="local\_desc01 local\_desc"><p><strong>캡챠파일 '.$cnt.'건의 삭제 완료됐습니다.</strong><br>프로그램의 실행을 끝마치셔도 좋습니다.</p></div>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" UPDATE `{$g5['config\_table']}` SET cf\_mobile\_pages = '5' ", true);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['uniqid\_table']}` (

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['autosave\_table']}` (

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['member\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['cert\_history\_table']}` (

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 183 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 189 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['visit\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 197 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query("ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 215 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query("ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 222 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query("ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 238 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['social\_profile\_table']}` (

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 258 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 264 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['member\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 270 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['member\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 276 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = "ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 282 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = "ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 288 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = "ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 293 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = "ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 298 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = "ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 339 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 357 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="3"><?php echo get\_member\_id\_select('cf\_admin', 10, $config['cf\_admin'], 'required') ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 375 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="3"><input type="checkbox" name="cf\_use\_point" value="1" id="cf\_use\_point" <?php echo $config['cf\_use\_point']?'checked':''; ?>> 사용</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 381 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_login\_point" value="<?php echo (int) $config['cf\_login\_point'] ?>" id="cf\_login\_point" required class="required frm\_input" size="5"> 점

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 386 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_memo\_send\_point" value="<?php echo (int) $config['cf\_memo\_send\_point']; ?>" id="cf\_memo\_send\_point" required class="required frm\_input" size="5"> 점

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 392 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_cut\_name" value="<?php echo (int) $config['cf\_cut\_name'] ?>" id="cf\_cut\_name" class="frm\_input" size="5"> 자리만 표시

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 397 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td>수정하면 <input type="text" name="cf\_nick\_modify" value="<?php echo (int) $config['cf\_nick\_modify'] ?>" id="cf\_nick\_modify" class="frm\_input" size="3"> 일 동안 바꿀 수 없음</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 399 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td>수정하면 <input type="text" name="cf\_open\_modify" value="<?php echo (int) $config['cf\_open\_modify'] ?>" id="cf\_open\_modify" class="frm\_input" size="3"> 일 동안 바꿀 수 없음</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 405 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_new\_del" value="<?php echo (int) $config['cf\_new\_del'] ?>" id="cf\_new\_del" class="frm\_input" size="5"> 일

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 410 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_memo\_del" value="<?php echo (int) $config['cf\_memo\_del'] ?>" id="cf\_memo\_del" class="frm\_input" size="5"> 일

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 417 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_visit\_del" value="<?php echo (int) $config['cf\_visit\_del'] ?>" id="cf\_visit\_del" class="frm\_input" size="5"> 일

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 422 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_popular\_del" value="<?php echo (int) $config['cf\_popular\_del'] ?>" id="cf\_popular\_del" class="frm\_input" size="5"> 일

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 429 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_login\_minutes" value="<?php echo (int) $config['cf\_login\_minutes'] ?>" id="cf\_login\_minutes" class="frm\_input" size="3"> 분

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 434 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_new\_rows" value="<?php echo (int) $config['cf\_new\_rows'] ?>" id="cf\_new\_rows" class="frm\_input" size="3"> 라인

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 441 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_page\_rows" value="<?php echo (int) $config['cf\_page\_rows'] ?>" id="cf\_page\_rows" class="frm\_input" size="3"> 라인

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 446 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_mobile\_page\_rows" value="<?php echo (int) $config['cf\_mobile\_page\_rows'] ?>" id="cf\_mobile\_page\_rows" class="frm\_input" size="3"> 라인

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 451 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="cf\_write\_pages" value="<?php echo (int) $config['cf\_write\_pages'] ?>" id="cf\_write\_pages" required class="required numeric frm\_input" size="3"> 페이지씩 표시</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 453 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="cf\_mobile\_pages" value="<?php echo (int) $config['cf\_mobile\_pages'] ?>" id="cf\_mobile\_pages" required class="required numeric frm\_input" size="3"> 페이지씩 표시</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 458 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_skin\_select('new', 'cf\_new\_skin', 'cf\_new\_skin', $config['cf\_new\_skin'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 462 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_mobile\_skin\_select('new', 'cf\_mobile\_new\_skin', 'cf\_mobile\_new\_skin', $config['cf\_mobile\_new\_skin'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 468 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_skin\_select('search', 'cf\_search\_skin', 'cf\_search\_skin', $config['cf\_search\_skin'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 472 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_mobile\_skin\_select('search', 'cf\_mobile\_search\_skin', 'cf\_mobile\_search\_skin', $config['cf\_mobile\_search\_skin'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 478 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_skin\_select('connect', 'cf\_connect\_skin', 'cf\_connect\_skin', $config['cf\_connect\_skin'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 482 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_mobile\_skin\_select('connect', 'cf\_mobile\_connect\_skin', 'cf\_mobile\_connect\_skin', $config['cf\_mobile\_connect\_skin'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 488 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_skin\_select('faq', 'cf\_faq\_skin', 'cf\_faq\_skin', $config['cf\_faq\_skin'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 492 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_mobile\_skin\_select('faq', 'cf\_mobile\_faq\_skin', 'cf\_mobile\_faq\_skin', $config['cf\_mobile\_faq\_skin'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 503 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo "<option value=\"\">사용안함</option>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 504 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<option value=\"".$arr[$i]."\"".get\_selected($config['cf\_editor'], $arr[$i]).">".$arr[$i]."</option>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 515 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="kcaptcha" <?php echo get\_selected($config['cf\_captcha'], 'kcaptcha') ; ?>>Kcaptcha</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 516 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="recaptcha" <?php echo get\_selected($config['cf\_captcha'], 'recaptcha') ; ?>>reCAPTCHA V2</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 517 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="recaptcha\_inv" <?php echo get\_selected($config['cf\_captcha'], 'recaptcha\_inv') ; ?>>Invisible reCAPTCHA</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 529 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo "<option value=\"\">선택</option>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 530 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<option value=\"".$arr[$i]."\"".get\_selected($config['cf\_captcha\_mp3'], $arr[$i]).">".$arr[$i]."</option>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 553 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_use\_copy\_log" value="1" id="cf\_use\_copy\_log" <?php echo $config['cf\_use\_copy\_log']?'checked':''; ?>> 남김

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 560 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_point\_term" value="<?php echo (int) $config['cf\_point\_term']; ?>" id="cf\_point\_term" required class="required frm\_input" size="5"> 일

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 579 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="cf\_analytics" id="cf\_analytics"><?php echo get\_text($config['cf\_analytics']); ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 586 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="cf\_add\_meta" id="cf\_add\_meta"><?php echo get\_text($config['cf\_add\_meta']); ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 612 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 629 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="cf\_delay\_sec" value="<?php echo (int) $config['cf\_delay\_sec'] ?>" id="cf\_delay\_sec" required class="required numeric frm\_input" size="3"> 초 지난후 가능</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 634 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="\_blank"<?php echo get\_selected($config['cf\_link\_target'], '\_blank') ?>>\_blank</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 635 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="\_self"<?php echo get\_selected($config['cf\_link\_target'], '\_self') ?>>\_self</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 636 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="\_top"<?php echo get\_selected($config['cf\_link\_target'], '\_top') ?>>\_top</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 637 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="\_new"<?php echo get\_selected($config['cf\_link\_target'], '\_new') ?>>\_new</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 643 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="cf\_read\_point" value="<?php echo (int) $config['cf\_read\_point'] ?>" id="cf\_read\_point" required class="required frm\_input" size="3"> 점</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 645 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="cf\_write\_point" value="<?php echo (int) $config['cf\_write\_point'] ?>" id="cf\_write\_point" required class="required frm\_input" size="3"> 점</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 649 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="cf\_comment\_point" value="<?php echo (int) $config['cf\_comment\_point'] ?>" id="cf\_comment\_point" required class="required frm\_input" size="3"> 점</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 651 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="cf\_download\_point" value="<?php echo (int) $config['cf\_download\_point'] ?>" id="cf\_download\_point" required class="required frm\_input" size="3"> 점</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 655 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="3"><input type="text" name="cf\_search\_part" value="<?php echo (int) $config['cf\_search\_part'] ?>" id="cf\_search\_part" class="frm\_input" size="4"> 건 단위로 검색</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 692 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 710 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_skin\_select('member', 'cf\_member\_skin', 'cf\_member\_skin', $config['cf\_member\_skin'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 714 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_mobile\_skin\_select('member', 'cf\_mobile\_member\_skin', 'cf\_mobile\_member\_skin', $config['cf\_mobile\_member\_skin'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 720 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_use\_homepage" value="1" id="cf\_use\_homepage" <?php echo $config['cf\_use\_homepage']?'checked':''; ?>> <label for="cf\_use\_homepage">보이기</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 721 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_req\_homepage" value="1" id="cf\_req\_homepage" <?php echo $config['cf\_req\_homepage']?'checked':''; ?>> <label for="cf\_req\_homepage">필수입력</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 725 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_use\_addr" value="1" id="cf\_use\_addr" <?php echo $config['cf\_use\_addr']?'checked':''; ?>> <label for="cf\_use\_addr">보이기</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 726 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_req\_addr" value="1" id="cf\_req\_addr" <?php echo $config['cf\_req\_addr']?'checked':''; ?>> <label for="cf\_req\_addr">필수입력</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 732 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_use\_tel" value="1" id="cf\_use\_tel" <?php echo $config['cf\_use\_tel']?'checked':''; ?>> <label for="cf\_use\_tel">보이기</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 733 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_req\_tel" value="1" id="cf\_req\_tel" <?php echo $config['cf\_req\_tel']?'checked':''; ?>> <label for="cf\_req\_tel">필수입력</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 737 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_use\_hp" value="1" id="cf\_use\_hp" <?php echo $config['cf\_use\_hp']?'checked':''; ?>> <label for="cf\_use\_hp">보이기</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 738 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_req\_hp" value="1" id="cf\_req\_hp" <?php echo $config['cf\_req\_hp']?'checked':''; ?>> <label for="cf\_req\_hp">필수입력</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 744 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_use\_signature" value="1" id="cf\_use\_signature" <?php echo $config['cf\_use\_signature']?'checked':''; ?>> <label for="cf\_use\_signature">보이기</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 745 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_req\_signature" value="1" id="cf\_req\_signature" <?php echo $config['cf\_req\_signature']?'checked':''; ?>> <label for="cf\_req\_signature">필수입력</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 749 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_use\_profile" value="1" id="cf\_use\_profile" <?php echo $config['cf\_use\_profile']?'checked':''; ?>> <label for="cf\_use\_profile">보이기</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 750 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_req\_profile" value="1" id="cf\_req\_profile" <?php echo $config['cf\_req\_profile']?'checked':''; ?>> <label for="cf\_req\_profile">필수입력</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 755 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_member\_level\_select('cf\_register\_level', 1, 9, $config['cf\_register\_level']) ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 757 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="cf\_register\_point" value="<?php echo (int) $config['cf\_register\_point'] ?>" id="cf\_register\_point" class="frm\_input" size="5"> 점</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 761 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="3"><input type="text" name="cf\_leave\_day" value="<?php echo (int) $config['cf\_leave\_day'] ?>" id="cf\_leave\_day" class="frm\_input" size="2"> 일 후 자동 삭제</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 768 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0"<?php echo get\_selected($config['cf\_use\_member\_icon'], '0') ?>>미사용

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 769 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"<?php echo get\_selected($config['cf\_use\_member\_icon'], '1') ?>>아이콘만 표시

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 770 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="2"<?php echo get\_selected($config['cf\_use\_member\_icon'], '2') ?>>아이콘+이름 표시

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 774 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_member\_level\_select('cf\_icon\_level', 1, 9, $config['cf\_icon\_level']) ?> 이상</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 778 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="cf\_member\_icon\_size" value="<?php echo (int) $config['cf\_member\_icon\_size'] ?>" id="cf\_member\_icon\_size" class="frm\_input" size="10"> 바이트 이하</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 782 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_member\_icon\_width" value="<?php echo (int) $config['cf\_member\_icon\_width'] ?>" id="cf\_member\_icon\_width" class="frm\_input" size="2">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 784 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_member\_icon\_height" value="<?php echo (int) $config['cf\_member\_icon\_height'] ?>" id="cf\_member\_icon\_height" class="frm\_input" size="2">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 790 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="cf\_member\_img\_size" value="<?php echo (int) $config['cf\_member\_img\_size'] ?>" id="cf\_member\_img\_size" class="frm\_input" size="10"> 바이트 이하</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 794 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_member\_img\_width" value="<?php echo (int) $config['cf\_member\_img\_width'] ?>" id="cf\_member\_img\_width" class="frm\_input" size="2">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 796 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_member\_img\_height" value="<?php echo (int) $config['cf\_member\_img\_height'] ?>" id="cf\_member\_img\_height" class="frm\_input" size="2">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 802 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="checkbox" name="cf\_use\_recommend" value="1" id="cf\_use\_recommend" <?php echo $config['cf\_use\_recommend']?'checked':''; ?>> 사용</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 804 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="cf\_recommend\_point" value="<?php echo (int) $config['cf\_recommend\_point'] ?>" id="cf\_recommend\_point" class="frm\_input"> 점</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 820 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="3"><textarea name="cf\_stipulation" id="cf\_stipulation" rows="10"><?php echo html\_purifier($config['cf\_stipulation']); ?></textarea></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 824 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="3"><textarea id="cf\_privacy" name="cf\_privacy" rows="10"><?php echo html\_purifier($config['cf\_privacy']); ?></textarea></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 835 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 856 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo option\_selected("0", $config['cf\_cert\_use'], "사용안함"); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 857 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo option\_selected("1", $config['cf\_cert\_use'], "테스트"); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 858 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo option\_selected("2", $config['cf\_cert\_use'], "실서비스"); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 874 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo option\_selected("", $config['cf\_cert\_simple'], "사용안함"); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 875 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo option\_selected("inicis", $config['cf\_cert\_simple'], "KG이니시스 통합인증(간편인증)"); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 883 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo option\_selected("", $config['cf\_cert\_hp'], "사용안함"); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 884 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo option\_selected("kcb", $config['cf\_cert\_hp'], "코리아크레딧뷰로(KCB) 휴대폰 본인확인"); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 885 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo option\_selected("kcp", $config['cf\_cert\_hp'], "NHN KCP 휴대폰 본인확인"); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 893 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo option\_selected("", $config['cf\_cert\_ipin'], "사용안함"); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 894 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo option\_selected("kcb", $config['cf\_cert\_ipin'], "코리아크레딧뷰로(KCB) 아이핀"); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 931 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_cert\_limit" value="<?php echo (int) $config['cf\_cert\_limit']; ?>" id="cf\_cert\_limit" class="frm\_input" size="3"> 회

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 938 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_cert\_req" value="1" id="cf\_cert\_req"<?php echo get\_checked($config['cf\_cert\_req'], 1); ?>> 예

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 952 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 966 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_email\_use" value="1" id="cf\_email\_use" <?php echo $config['cf\_email\_use']?'checked':''; ?>> 사용

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 973 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo help('메일에 배달된 인증 주소를 클릭하여야 회원으로 인정합니다.'.$tmp); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 974 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_use\_email\_certify" value="1" id="cf\_use\_email\_certify" <?php echo $config['cf\_use\_email\_certify']?'checked':''; ?>> 사용

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 981 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_formmail\_is\_member" value="1" id="cf\_formmail\_is\_member" <?php echo $config['cf\_formmail\_is\_member']?'checked':''; ?>> 회원만 사용

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 991 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1005 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_email\_wr\_super\_admin" value="1" id="cf\_email\_wr\_super\_admin" <?php echo $config['cf\_email\_wr\_super\_admin']?'checked':''; ?>> 사용

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1012 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_email\_wr\_group\_admin" value="1" id="cf\_email\_wr\_group\_admin" <?php echo $config['cf\_email\_wr\_group\_admin']?'checked':''; ?>> 사용

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1019 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_email\_wr\_board\_admin" value="1" id="cf\_email\_wr\_board\_admin" <?php echo $config['cf\_email\_wr\_board\_admin']?'checked':''; ?>> 사용

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1026 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_email\_wr\_write" value="1" id="cf\_email\_wr\_write" <?php echo $config['cf\_email\_wr\_write']?'checked':''; ?>> 사용

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1033 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_email\_wr\_comment\_all" value="1" id="cf\_email\_wr\_comment\_all" <?php echo $config['cf\_email\_wr\_comment\_all']?'checked':''; ?>> 사용

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1044 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1058 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_email\_mb\_super\_admin" value="1" id="cf\_email\_mb\_super\_admin" <?php echo $config['cf\_email\_mb\_super\_admin']?'checked':''; ?>> 사용

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1065 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_email\_mb\_member" value="1" id="cf\_email\_mb\_member" <?php echo $config['cf\_email\_mb\_member']?'checked':''; ?>> 사용

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1076 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1090 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_email\_po\_super\_admin" value="1" id="cf\_email\_po\_super\_admin" <?php echo $config['cf\_email\_po\_super\_admin']?'checked':''; ?>> 사용

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_social\_login\_use" value="1" id="cf\_social\_login\_use" <?php echo (!empty($config['cf\_social\_login\_use']))?'checked':''; ?>> 사용

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_social\_servicelist[]" id="check\_social\_naver" value="naver" <?php echo option\_array\_checked('naver', $config['cf\_social\_servicelist']); ?> >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_social\_servicelist[]" id="check\_social\_kakao" value="kakao" <?php echo option\_array\_checked('kakao', $config['cf\_social\_servicelist']); ?> >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_social\_servicelist[]" id="check\_social\_facebook" value="facebook" <?php echo option\_array\_checked('facebook', $config['cf\_social\_servicelist']); ?> >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_social\_servicelist[]" id="check\_social\_google" value="google" <?php echo option\_array\_checked('google', $config['cf\_social\_servicelist']); ?> >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_social\_servicelist[]" id="check\_social\_twitter" value="twitter" <?php echo option\_array\_checked('twitter', $config['cf\_social\_servicelist']); ?> >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_social\_servicelist[]" id="check\_social\_payco" value="payco" <?php echo option\_array\_checked('payco', $config['cf\_social\_servicelist']); ?> >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1253 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1270 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="cf\_add\_script" id="cf\_add\_script"><?php echo get\_text($config['cf\_add\_script']); ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1281 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1295 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="" <?php echo get\_selected($config['cf\_sms\_use'], ''); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1296 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="icode" <?php echo get\_selected($config['cf\_sms\_use'], 'icode'); ?>>아이코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1305 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="" <?php echo get\_selected($config['cf\_sms\_type'], ''); ?>>SMS</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1306 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="LMS" <?php echo get\_selected($config['cf\_sms\_type'], 'LMS'); ?>>LMS</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1324 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="icode\_old\_version <?php if(!(isset($userinfo['payment']) && $userinfo['payment'])){ echo 'cf\_tr\_hide'; } ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1346 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo number\_format($userinfo['coin']); ?> 원.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1347 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="http://www.icodekorea.com/smsbiz/credit\_card\_amt.php?icode\_id=<?php echo get\_text($config['cf\_icode\_id']); ?>&amp;icode\_passwd=<?php echo get\_text($config['cf\_icode\_pw']); ?>" target="\_blank" class="btn\_frmline">충전하기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1358 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

서버아이피 : <?php echo $\_SERVER['SERVER\_ADDR']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1375 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1390 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row">여분필드<?php echo $i ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1392 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="cf\_<?php echo $i ?>\_subj">여분필드<?php echo $i ?> 제목</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1393 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_<?php echo $i ?>\_subj" value="<?php echo get\_text($config['cf\_'.$i.'\_subj']) ?>" id="cf\_<?php echo $i ?>\_subj" class="frm\_input" size="30">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1394 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="cf\_<?php echo $i ?>">여분필드<?php echo $i ?> 값</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1414 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$(".cf\_cert\_service").addClass("cf\_cert\_hide");';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1474 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var current\_user\_ip = "<?php echo $\_SERVER['REMOTE\_ADDR']; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1517 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo module\_exec\_check($exe, 'okname');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1535 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo module\_exec\_check($exe, 'ct\_cli');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1563 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'alert("'.str\_replace(G5\_PATH.'/', '',$log\_path).' 폴더에 쓰기권한을 부여해 주십시오.\n> chmod 707 log");'.PHP\_EOL;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$posts[$key] = $\_POST[$key] = preg\_replace('/[^a-z0-9\_\-\.]/i', '', $\_POST[$key]);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\config\_form\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$posts['cf\_icode\_server\_port'] = $\_POST['cf\_icode\_server\_port'] = isset($\_POST['cf\_icode\_server\_port']) ? preg\_replace('/[^0-9]/', '', $\_POST['cf\_icode\_server\_port']) : '7295';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$co\_id = isset($\_REQUEST['co\_id']) ? preg\_replace('/[^a-z0-9\_]/i', '', $\_REQUEST['co\_id']) : '';

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " ALTER TABLE `{$g5['content\_table']}` ADD `co\_include\_head` VARCHAR( 255 ) NOT NULL ,

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['content\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['content\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['content\_table']}`

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" value="<?php echo $co['co\_id']; ?>" name="co\_id" id ="co\_id" required <?php echo $readonly; ?> class="required <?php echo $readonly; ?> frm\_input" size="20" maxlength="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($w == 'u') { ?><a href="<?php echo get\_pretty\_url('content', $co\_id); ?>" class="btn\_frmline">내용확인</a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="co\_subject" value="<?php echo htmlspecialchars2($co['co\_subject']); ?>" id="co\_subject" required class="frm\_input required" size="90"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo editor\_html('co\_content', get\_text(html\_purifier($co['co\_content']), 0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo editor\_html('co\_mobile\_content', get\_text(html\_purifier($co['co\_mobile\_content']), 0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_skin\_select('content', 'co\_skin', 'co\_skin', $co['co\_skin'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_mobile\_skin\_select('content', 'co\_mobile\_skin', 'co\_mobile\_skin', $co['co\_mobile\_skin'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"<?php echo get\_selected($co['co\_tag\_filter\_use'], 1); ?>>사용함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0"<?php echo get\_selected($co['co\_tag\_filter\_use'], 0); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="co\_include\_head" value="<?php echo $co['co\_include\_head']; ?>" id="co\_include\_head" class="frm\_input" size="60">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="co\_include\_tail" value="<?php echo $co['co\_include\_tail']; ?>" id="co\_include\_tail" class="frm\_input" size="60">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $captcha\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $himg\_str;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 203 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $timg\_str;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 240 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var co\_include\_head = "<?php echo $co['co\_include\_head']; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 241 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var co\_include\_tail = "<?php echo $co['co\_include\_tail']; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 290 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_js;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$co\_id = isset($\_REQUEST['co\_id']) ? preg\_replace('/[^a-z0-9\_]/i', '', $\_REQUEST['co\_id']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$co\_include\_head = isset($\_POST['co\_include\_head']) ? preg\_replace(array("#[\\\]+$#", "#(<\?php|<\?)#i"), "", substr($\_POST['co\_include\_head'], 0, 255)) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$co\_include\_tail = isset($\_POST['co\_include\_tail']) ? preg\_replace(array("#[\\\]+$#", "#(<\?php|<\?)#i"), "", substr($\_POST['co\_include\_tail'], 0, 255)) : '';

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentlist.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE {$g5['g5\_shop\_content\_table']} RENAME TO `{$g5['content\_table']}` ;", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentlist.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$query\_cp = sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['content\_table']}` (

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentlist.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" insert into `{$g5['content\_table']}` set co\_id = 'company', co\_html = '1', co\_subject = '회사소개', co\_content= '<p align=center><b>회사소개에 대한 내용을 입력하십시오.</b></p>' ", false );

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentlist.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" insert into `{$g5['content\_table']}` set co\_id = 'privacy', co\_html = '1', co\_subject = '개인정보 처리방침', co\_content= '<p align=center><b>개인정보 처리방침에 대한 내용을 입력하십시오.</b></p>' ", false );

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentlist.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" insert into `{$g5['content\_table']}` set co\_id = 'provision', co\_html = '1', co\_subject = '서비스 이용약관', co\_content= '<p align=center><b>서비스 이용약관에 대한 내용을 입력하십시오.</b></p>' ", false );

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($page > 1) {?><a href="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">처음으로</a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">전체 내용</span><span class="ov\_num"> <?php echo $total\_count; ?>건</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_id"><?php echo $row['co\_id']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><?php echo htmlspecialchars2($row['co\_subject']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./contentform.php?w=u&amp;co\_id=<?php echo $row['co\_id']; ?>" class="btn btn\_03"><span class="sound\_only"><?php echo htmlspecialchars2($row['co\_subject']); ?> </span>수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url('content', $row['co\_id']); ?>" class="btn btn\_02"><span class="sound\_only"><?php echo htmlspecialchars2($row['co\_subject']); ?> </span> 보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./contentformupdate.php?w=d&amp;co\_id=<?php echo $row['co\_id']; ?>" onclick="return delete\_confirm(this);" class="btn btn\_02"><span class="sound\_only"><?php echo htmlspecialchars2($row['co\_subject']); ?> </span>삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\contentlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query("ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query("ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query("ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['social\_profile\_table']}` (

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query("ALTER TABLE `{$write\_table}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " SHOW COLUMNS FROM `{$g5['content\_table']}` LIKE 'co\_seo\_title' ";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query("ALTER TABLE `{$g5['content\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " SHOW COLUMNS FROM `{$g5['memo\_table']}` LIKE 'me\_send\_id' ";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query("ALTER TABLE `{$g5['memo\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['member\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['member\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 160 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " SHOW COLUMNS FROM `{$g5['board\_file\_table']}` LIKE 'bf\_fileurl' ";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 172 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['board\_file\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 183 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['g5\_shop\_post\_log\_table']}` (

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 198 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$result = sql\_query("describe `{$g5['g5\_shop\_post\_log\_table']}`");

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 201 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query("ALTER TABLE `{$g5['g5\_shop\_post\_log\_table']}` MODIFY ol\_msg TEXT NOT NULL;", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 202 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query("ALTER TABLE `{$g5['g5\_shop\_post\_log\_table']}` DROP PRIMARY KEY;", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 203 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query("ALTER TABLE `{$g5['g5\_shop\_post\_log\_table']}` ADD `log\_id` int(11) NOT NULL AUTO\_INCREMENT, ADD PRIMARY KEY (`log\_id`);", false);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 217 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\dbupgrade.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $db\_upgrade\_msg; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fm\_id" value="<?php echo $fm\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fa\_id" value="<?php echo $fa\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="fa\_order" value="<?php echo $fa['fa\_order']; ?>" id="fa\_order" class="frm\_input" maxlength="10" size="10">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($w == 'u') { ?><a href="<?php echo G5\_BBS\_URL; ?>/faq.php?fm\_id=<?php echo $fm\_id; ?>" class="btn\_frmline">내용보기</a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo editor\_html('fa\_subject', get\_text(html\_purifier($fa['fa\_subject']), 0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo editor\_html('fa\_content', get\_text(html\_purifier($fa['fa\_content']), 0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./faqlist.php?fm\_id=<?php echo $fm\_id; ?>" class="btn btn\_02">목록</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt"> 등록된 FAQ 상세내용</span><span class="ov\_num"> <?php echo $total\_count; ?>건</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./faqform.php?fm\_id=<?php echo $fm['fm\_id']; ?>" class="btn btn\_01">FAQ 상세내용 추가</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $num; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><?php echo $fa\_subject; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['fa\_order']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./faqform.php?w=u&amp;fm\_id=<?php echo $row['fm\_id']; ?>&amp;fa\_id=<?php echo $row['fa\_id']; ?>" class="btn btn\_03"><span class="sound\_only"><?php echo $fa\_subject; ?> </span>수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./faqformupdate.php?w=d&amp;fm\_id=<?php echo $row['fm\_id']; ?>&amp;fa\_id=<?php echo $row['fa\_id']; ?>" onclick="return delete\_confirm(this);" class="btn btn\_02"><span class="sound\_only"><?php echo $fa\_subject; ?> </span>삭제</a>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fm\_id = isset($\_GET['fm\_id']) ? preg\_replace('/[^0-9]/', '', $\_GET['fm\_id']) : 0;

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['faq\_master\_table']}`

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fm\_id" value="<?php echo $fm\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="fm\_order" value="<?php echo $fm['fm\_order']; ?>" id="fm\_order" class="frm\_input" maxlength="10" size="10">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" value="<?php echo get\_text($fm['fm\_subject']); ?>" name="fm\_subject" id="fm\_subject" required class="frm\_input required" size="70">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_BBS\_URL; ?>/faq.php?fm\_id=<?php echo $fm\_id; ?>" class="btn\_frmline">보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./faqlist.php?fm\_id=<?php echo $fm\_id; ?>" class="btn\_frmline">상세보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $himg\_str;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $timg\_str;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo editor\_html('fm\_head\_html', get\_text(html\_purifier($fm['fm\_head\_html']), 0)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo editor\_html('fm\_tail\_html', get\_text(html\_purifier($fm['fm\_tail\_html']), 0)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo editor\_html('fm\_mobile\_head\_html', get\_text(html\_purifier($fm['fm\_mobile\_head\_html']), 0)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo editor\_html('fm\_mobile\_tail\_html', get\_text(html\_purifier($fm['fm\_mobile\_tail\_html']), 0)); ?>

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterlist.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE {$g5['g5\_shop\_faq\_master\_table']} RENAME TO `{$g5['faq\_master\_table']}` ;", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterlist.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$query\_cp = sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['faq\_master\_table']}` (

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterlist.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" insert into `{$g5['faq\_master\_table']}` set fm\_id = '1', fm\_subject = '자주하시는 질문' ", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterlist.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE {$g5['g5\_shop\_faq\_table']} RENAME TO `{$g5['faq\_table']}` ;", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterlist.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$query\_cp = sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['faq\_table']}` (

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($page > 1) {?><a href="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">처음으로</a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt"> 전체 FAQ </span><span class="ov\_num"> <?php echo $total\_count; ?>건</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['fm\_id']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><a href="./faqlist.php?fm\_id=<?php echo $row['fm\_id']; ?>&amp;fm\_subject=<?php echo $row['fm\_subject']; ?>"><?php echo stripslashes($row['fm\_subject']); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $cnt; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['fm\_order']?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./faqmasterform.php?w=u&amp;fm\_id=<?php echo $row['fm\_id']; ?>" class="btn btn\_03"><span class="sound\_only"><?php echo stripslashes($row['fm\_subject']); ?> </span>수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_BBS\_URL; ?>/faq.php?fm\_id=<?php echo $row['fm\_id']; ?>" class="btn btn\_02"><span class="sound\_only"><?php echo stripslashes($row['fm\_subject']); ?> </span>보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./faqmasterformupdate.php?w=d&amp;fm\_id=<?php echo $row['fm\_id']; ?>" onclick="return delete\_confirm(this);" class="btn btn\_02"><span class="sound\_only"><?php echo stripslashes($row['fm\_subject']); ?> </span>삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\faqmasterlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2>신규가입회원 <?php echo $new\_member\_rows ?>건 목록</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

총회원수 <?php echo number\_format($total\_count) ?>명 중 차단 <?php echo number\_format($intercept\_count) ?>명, 탈퇴 : <?php echo number\_format($leave\_count) ?>명

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbid"><?php echo $mb\_id ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbname"><?php echo get\_text($row['mb\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbname sv\_use"><div><?php echo $mb\_nick ?></div></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['mb\_level'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><a href="./point\_list.php?sfl=mb\_id&amp;stx=<?php echo $row['mb\_id'] ?>"><?php echo number\_format($row['mb\_point']) ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_boolean"><?php echo $row['mb\_mailling']?'예':'아니오'; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_boolean"><?php echo $row['mb\_open']?'예':'아니오'; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_boolean"><?php echo preg\_match('/[1-9]/', $row['mb\_email\_certify'])?'예':'아니오'; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_boolean"><?php echo $row['mb\_intercept\_date']?'예':'아니오'; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_category"><?php echo $group ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 209 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_category"><a href="<?php echo G5\_BBS\_URL ?>/new.php?gr\_id=<?php echo $row['gr\_id'] ?>"><?php echo cut\_str($row['gr\_subject'],10) ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 210 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_category"><a href="<?php echo get\_pretty\_url($row['bo\_table']) ?>"><?php echo cut\_str($row['bo\_subject'],20) ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 211 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><a href="<?php echo get\_pretty\_url($row['bo\_table'], $row2['wr\_id']); ?><?php echo $comment\_link ?>"><?php echo $comment ?><?php echo conv\_subject($row2['wr\_subject'], 100) ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 212 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbname"><div><?php echo $name ?></div></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 213 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo $datetime ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 219 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 248 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

전체 <?php echo number\_format($total\_count) ?> 건 중 <?php echo $new\_point\_rows ?>건 목록

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 287 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbid"><a href="./point\_list.php?sfl=mb\_id&amp;stx=<?php echo $row['mb\_id'] ?>"><?php echo $row['mb\_id'] ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 288 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbname"><?php echo get\_text($row2['mb\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 289 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_name sv\_use"><div><?php echo $mb\_nick ?></div></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 290 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo $row['po\_datetime'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 291 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $link1.$row['po\_content'].$link2 ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 292 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig"><?php echo number\_format($row['po\_point']) ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 293 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig"><?php echo number\_format($row['po\_mb\_point']) ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 300 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>" id="w">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ma\_id" value="<?php echo $ma['ma\_id'] ?>" id="ma\_id">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo editor\_html("ma\_content", get\_text(html\_purifier($ma['ma\_content']), 0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

현재 등록된 메일은 총 <?php echo $total\_count ?>건입니다.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i; ?>" class="sound\_only"><?php echo $row['ma\_subject']; ?> 메일</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="chk\_<?php echo $i ?>" name="chk[]" value="<?php echo $row['ma\_id'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_c"><?php echo $num ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><a href="./mail\_form.php?w=u&amp;ma\_id=<?php echo $row['ma\_id'] ?>"><?php echo $row['ma\_subject'] ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo $row['ma\_time'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_test"><a href="./mail\_test.php?ma\_id=<?php echo $row['ma\_id'] ?>">테스트</a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_send"><a href="./mail\_select\_form.php?ma\_id=<?php echo $row['ma\_id'] ?>">보내기</a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mng"><?php echo $s\_vie ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<tr><td colspan=\"".$colspan."\" class=\"empty\_table\">자료가 없습니다.</td></tr>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_preview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $subject; ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_preview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $content; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

전체회원 <?php echo number\_format($tot\_cnt) ?>명 , 탈퇴대기회원 <?php echo number\_format($finish\_cnt) ?>명, 정상회원 <?php echo number\_format($tot\_cnt - $finish\_cnt) ?>명 중 메일 발송 대상 선택

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ma\_id" value="<?php echo $ma\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 대상선택</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="mb\_id1" value="1" id="mb\_id1\_all" <?php echo $mb\_id1?"checked":""; ?>> <label for="mb\_id1\_all">전체</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="mb\_id1" value="0" id="mb\_id1\_section" <?php echo !$mb\_id1?"checked":""; ?>> <label for="mb\_id1\_section">구간</label>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_form.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

<?php echo help("메일 주소에 단어 포함 (예 : @".preg\_replace('#^(www[^\.]\*\.){1}#', '', $\_SERVER['HTTP\_HOST']).")") ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo help("메일 주소에 단어 포함 (예 : @".preg\_replace('#^(www[^\.]\*\.){1}#', '', $\_SERVER['HTTP\_HOST']).")") ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $i ?>"><?php echo $i ?></option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $i ?>"<?php echo $i==10 ? " selected" : ""; ?>><?php echo $i ?></option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<option value="'.$row['gr\_id'].'">'.$row['gr\_subject'].'</option>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ma\_id" value="<?php echo $ma\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $i ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbid"><?php echo $row['mb\_id'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbname"><?php echo get\_text($row['mb\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbname"><?php echo $row['mb\_nick'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $row['mb\_email'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="ma\_list" style="display:none"><?php echo $ma\_list?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./mail\_select\_form.php?ma\_id=<?php echo $ma\_id ?>">뒤로</a>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_update.php

MD5 Hashing algorithm.

$mb\_md5 = md5($mb\_id.$to\_email.$datetime);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$content = preg\_replace("/{이름}/", $name, $content);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$content = preg\_replace("/{닉네임}/", $nick, $content);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$content = preg\_replace("/{회원아이디}/", $mb\_id, $content);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$content = preg\_replace("/{이메일}/", $to\_email, $content);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_update.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<script> document.all.cont.innerHTML += '$cnt. $to\_email ($mb\_id : $name)<br>'; </script>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_select\_update.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<script> document.all.cont.innerHTML += "<br><br>총 <?php echo number\_format($cnt) ?>건 발송<br><br><font color=crimson><b>[끝]</b></font>"; document.body.scrollTop += 1000; </script>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_test.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$content = preg\_replace("/{이름}/", $name, $content);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_test.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$content = preg\_replace("/{닉네임}/", $nick, $content);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_test.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$content = preg\_replace("/{회원아이디}/", $mb\_id, $content);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_test.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$content = preg\_replace("/{이메일}/", $email, $content);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\mail\_test.php

MD5 Hashing algorithm.

$mb\_md5 = md5($member['mb\_id'].$member['mb\_email'].$member['mb\_datetime']);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['member\_table']}` DROP `mb\_certify` ", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['member\_table']}` ADD `mb\_certify` TINYINT(4) NOT NULL DEFAULT '0' AFTER `mb\_hp` ", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['member\_table']}` CHANGE `mb\_adult` `mb\_adult` TINYINT(4) NOT NULL DEFAULT '0' ", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['member\_table']}` ADD `mb\_adult` TINYINT NOT NULL DEFAULT '0' AFTER `mb\_certify` ", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 182 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['member\_cert\_history\_table']}` (

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 211 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 212 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 213 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 214 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 215 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 216 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 221 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 230 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><label for="mb\_id">아이디<?php echo $sound\_only ?></label></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 232 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_id" value="<?php echo $mb['mb\_id'] ?>" id="mb\_id" <?php echo $required\_mb\_id ?> class="frm\_input <?php echo $required\_mb\_id\_class ?>" size="15" maxlength="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 233 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($w=='u'){ ?><a href="./boardgroupmember\_form.php?mb\_id=<?php echo $mb['mb\_id'] ?>" class="btn\_frmline">접근가능그룹보기</a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 235 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><label for="mb\_password">비밀번호<?php echo $sound\_only ?></label></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="password" name="mb\_password" id="mb\_password" <?php echo $required\_mb\_password ?> class="frm\_input <?php echo $required\_mb\_password ?>" size="15" maxlength="20"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 240 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="mb\_name" value="<?php echo $mb['mb\_name'] ?>" id="mb\_name" required class="required frm\_input" size="15" maxlength="20"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 242 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="mb\_nick" value="<?php echo $mb['mb\_nick'] ?>" id="mb\_nick" required class="required frm\_input" size="15" maxlength="20"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 246 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_member\_level\_select('mb\_level', 1, $member['mb\_level'], $mb['mb\_level']) ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 248 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><a href="./point\_list.php?sfl=mb\_id&amp;stx=<?php echo $mb['mb\_id'] ?>" target="\_blank"><?php echo number\_format($mb['mb\_point']) ?></a> 점</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 252 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="mb\_email" value="<?php echo $mb['mb\_email'] ?>" id="mb\_email" maxlength="100" required class="required frm\_input email" size="30"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 254 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="mb\_homepage" value="<?php echo $mb['mb\_homepage'] ?>" id="mb\_homepage" class="frm\_input" maxlength="255" size="15"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 258 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="mb\_hp" value="<?php echo $mb['mb\_hp'] ?>" id="mb\_hp" class="frm\_input" size="15" maxlength="20"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 260 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="mb\_tel" value="<?php echo $mb['mb\_tel'] ?>" id="mb\_tel" class="frm\_input" size="15" maxlength="20"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 265 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="mb\_certify\_case" value="simple" id="mb\_certify\_sa" <?php if($mb['mb\_certify'] == 'simple') echo 'checked="checked"'; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 267 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="mb\_certify\_case" value="hp" id="mb\_certify\_hp" <?php if($mb['mb\_certify'] == 'hp') echo 'checked="checked"'; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 269 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="mb\_certify\_case" value="ipin" id="mb\_certify\_ipin" <?php if($mb['mb\_certify'] == 'ipin') echo 'checked="checked"'; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 276 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="mb\_certify" value="1" id="mb\_certify\_yes" <?php echo $mb\_certify\_yes; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 278 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="mb\_certify" value="" id="mb\_certify\_no" <?php echo $mb\_certify\_no; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 283 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="mb\_adult" value="1" id="mb\_adult\_yes" <?php echo $mb\_adult\_yes; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 285 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="mb\_adult" value="0" id="mb\_adult\_no" <?php echo $mb\_adult\_no; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 293 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_zip" value="<?php echo $mb['mb\_zip1'].$mb['mb\_zip2']; ?>" id="mb\_zip" class="frm\_input readonly" size="5" maxlength="6">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 295 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_addr1" value="<?php echo $mb['mb\_addr1'] ?>" id="mb\_addr1" class="frm\_input readonly" size="60">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 297 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_addr2" value="<?php echo $mb['mb\_addr2'] ?>" id="mb\_addr2" class="frm\_input" size="60">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 300 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_addr3" value="<?php echo $mb['mb\_addr3'] ?>" id="mb\_addr3" class="frm\_input" size="60">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 302 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_addr\_jibeon" value="<?php echo $mb['mb\_addr\_jibeon']; ?>"><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 308 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo help('이미지 크기는 <strong>넓이 '.$config['cf\_member\_icon\_width'].'픽셀 높이 '.$config['cf\_member\_icon\_height'].'픽셀</strong>로 해주세요.') ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 316 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<img src="'.$icon\_url.$icon\_filemtile.'" alt="">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 325 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo help('이미지 크기는 <strong>넓이 '.$config['cf\_member\_img\_width'].'픽셀 높이 '.$config['cf\_member\_img\_height'].'픽셀</strong>로 해주세요.') ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 331 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_member\_profile\_img($mb['mb\_id']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 340 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="mb\_mailling" value="1" id="mb\_mailling\_yes" <?php echo $mb\_mailling\_yes; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 342 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="mb\_mailling" value="0" id="mb\_mailling\_no" <?php echo $mb\_mailling\_no; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 347 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="mb\_sms" value="1" id="mb\_sms\_yes" <?php echo $mb\_sms\_yes; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 349 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="mb\_sms" value="0" id="mb\_sms\_no" <?php echo $mb\_sms\_no; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 356 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="mb\_open" value="1" id="mb\_open\_yes" <?php echo $mb\_open\_yes; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 358 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="mb\_open" value="0" id="mb\_open\_no" <?php echo $mb\_open\_no; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 364 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="3"><textarea name="mb\_signature" id="mb\_signature"><?php echo $mb['mb\_signature'] ?></textarea></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 368 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="3"><textarea name="mb\_profile" id="mb\_profile"><?php echo $mb['mb\_profile'] ?></textarea></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 372 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="3"><textarea name="mb\_memo" id="mb\_memo"><?php echo $mb['mb\_memo'] ?></textarea></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 394 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

[<?php echo $row['ch\_datetime']; ?>]

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 395 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $row['mb\_id']; ?> /

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 396 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $row['ch\_name']; ?> /

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 397 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $row['ch\_hp']; ?> /

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 398 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $cert\_type; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 411 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $mb['mb\_datetime'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 413 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $mb['mb\_today\_login'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 417 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="3"><?php echo $mb['mb\_ip'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 428 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $mb['mb\_email\_certify'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 438 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="3"><?php echo ($mb['mb\_recommend'] ? get\_text($mb['mb\_recommend']) : '없음');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 445 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_leave\_date" value="<?php echo $mb['mb\_leave\_date'] ?>" id="mb\_leave\_date" class="frm\_input" maxlength="8">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 452 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_intercept\_date" value="<?php echo $mb['mb\_intercept\_date'] ?>" id="mb\_intercept\_date" class="frm\_input" maxlength="8">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 477 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="account\_provider" data-mpno="social\_<?php echo $account['mp\_no'];?>" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 479 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sns-icon sns-<?php echo $provider; ?>" title="<?php echo $provider\_name; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 481 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="txt"><?php echo $provider\_name; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 484 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="provider\_name"><?php echo $provider\_name;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 485 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="account\_hidden" style="display:none"><?php echo $account['mb\_id']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 487 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="btn\_info"><a href="<?php echo G5\_SOCIAL\_LOGIN\_URL.'/unlink.php?mp\_no='.$account['mp\_no'] ?>" class="social\_unlink" data-provider="<?php echo $account['mp\_no'];?>" >연동해제</a> <span class="sound\_only"><?php echo substr($account['mp\_register\_day'], 2, 14); ?></span></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 552 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><label for="mb\_<?php echo $i ?>">여분 필드 <?php echo $i ?></label></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 553 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="3"><input type="text" name="mb\_<?php echo $i ?>" value="<?php echo $mb['mb\_'.$i] ?>" id="mb\_<?php echo $i ?>" class="frm\_input" size="30" maxlength="255"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 562 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./member\_list.php?<?php echo $qstr ?>" class="btn btn\_02">목록</a>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$mb\_certify\_case = isset($\_POST['mb\_certify\_case']) ? preg\_replace('/[^0-9a-z\_]/i', '', $\_POST['mb\_certify\_case']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$mb\_certify = isset($\_POST['mb\_certify']) ? preg\_replace('/[^0-9a-z\_]/i', '', $\_POST['mb\_certify']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$mb\_zip = isset($\_POST['mb\_zip']) ? preg\_replace('/[^0-9a-z\_]/i', '', $\_POST['mb\_zip']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$mb\_certify = isset($\_POST['mb\_certify\_case']) ? preg\_replace('/[^0-9a-z\_]/i', '', $\_POST['mb\_certify\_case']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$mb\_adult = isset($\_POST['mb\_adult']) ? preg\_replace('/[^0-9a-z\_]/i', '', $\_POST['mb\_adult']) : '';

**MEDIUM: Potentially Unsafe Code - Code Appears to Contain Hard-Coded Password**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_form\_update.php

The code may contain a hard-coded password which an attacker could obtain from the source or by dis-assembling the executable. Please manually review the code:

$sql\_password = " , mb\_password = '".get\_encrypt\_string($mb\_password)."' ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">총회원수 </span><span class="ov\_num"> <?php echo number\_format($total\_count) ?>명 </span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="?sst=mb\_intercept\_date&amp;sod=desc&amp;sfl=<?php echo $sfl ?>&amp;stx=<?php echo $stx ?>" class="btn\_ov01" data-tooltip-text="차단된 순으로 정렬합니다.&#xa;전체 데이터를 출력합니다."> <span class="ov\_txt">차단 </span><span class="ov\_num"><?php echo number\_format($intercept\_count) ?>명</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="?sst=mb\_leave\_date&amp;sod=desc&amp;sfl=<?php echo $sfl ?>&amp;stx=<?php echo $stx ?>" class="btn\_ov01" data-tooltip-text="탈퇴된 순으로 정렬합니다.&#xa;전체 데이터를 출력합니다."> <span class="ov\_txt">탈퇴 </span><span class="ov\_num"><?php echo number\_format($leave\_count) ?>명</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mb\_id"<?php echo get\_selected($sfl, "mb\_id"); ?>>회원아이디</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mb\_nick"<?php echo get\_selected($sfl, "mb\_nick"); ?>>닉네임</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mb\_name"<?php echo get\_selected($sfl, "mb\_name"); ?>>이름</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mb\_level"<?php echo get\_selected($sfl, "mb\_level"); ?>>권한</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mb\_email"<?php echo get\_selected($sfl, "mb\_email"); ?>>E-MAIL</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mb\_tel"<?php echo get\_selected($sfl, "mb\_tel"); ?>>전화번호</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mb\_hp"<?php echo get\_selected($sfl, "mb\_hp"); ?>>휴대폰번호</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mb\_point"<?php echo get\_selected($sfl, "mb\_point"); ?>>포인트</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mb\_datetime"<?php echo get\_selected($sfl, "mb\_datetime"); ?>>가입일시</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mb\_ip"<?php echo get\_selected($sfl, "mb\_ip"); ?>>IP</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mb\_recommend"<?php echo get\_selected($sfl, "mb\_recommend"); ?>>추천인</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx ?>" id="stx" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 212 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 214 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id[<?php echo $i ?>]" value="<?php echo $row['mb\_id'] ?>" id="mb\_id\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 215 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i; ?>" class="sound\_only"><?php echo get\_text($row['mb\_name']); ?> <?php echo get\_text($row['mb\_nick']); ?>님</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 216 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk[]" value="<?php echo $i ?>" id="chk\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 219 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $mb\_id ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 232 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<span class="sns-icon sns-'.$provider.'" title="'.$provider\_name.'">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 234 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<span class="txt">'.$provider\_name.'</span>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 243 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="mb\_certify[<?php echo $i; ?>]" value="simple" id="mb\_certify\_sa\_<?php echo $i; ?>" <?php echo $row['mb\_certify']=='simple'?'checked':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 244 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="mb\_certify\_sa\_<?php echo $i; ?>">간편인증</label><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 245 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="mb\_certify[<?php echo $i; ?>]" value="hp" id="mb\_certify\_hp\_<?php echo $i; ?>" <?php echo $row['mb\_certify']=='hp'?'checked':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 246 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="mb\_certify\_hp\_<?php echo $i; ?>">휴대폰</label><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 247 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="mb\_certify[<?php echo $i; ?>]" value="ipin" id="mb\_certify\_ipin\_<?php echo $i; ?>" <?php echo $row['mb\_certify']=='ipin'?'checked':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 248 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="mb\_certify\_ipin\_<?php echo $i; ?>">아이핀</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 250 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="mb\_list\_mailc"><?php echo preg\_match('/[1-9]/', $row['mb\_email\_certify'])?'<span class="txt\_true">Yes</span>':'<span class="txt\_false">No</span>'; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 252 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="mb\_open\_<?php echo $i; ?>" class="sound\_only">정보공개</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 253 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="mb\_open[<?php echo $i; ?>]" <?php echo $row['mb\_open']?'checked':''; ?> value="1" id="mb\_open\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 256 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="mb\_mailling\_<?php echo $i; ?>" class="sound\_only">메일수신</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 257 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="mb\_mailling[<?php echo $i; ?>]" <?php echo $row['mb\_mailling']?'checked':''; ?> value="1" id="mb\_mailling\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 261 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($leave\_msg || $intercept\_msg) echo $leave\_msg.' '.$intercept\_msg;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 265 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="mb\_list\_mobile" class="td\_tel"><?php echo get\_text($row['mb\_hp']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 266 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="mb\_list\_lastcall" class="td\_date"><?php echo substr($row['mb\_today\_login'],2,8); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 267 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="mb\_list\_grp" class="td\_numsmall"><?php echo $group ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 268 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="mb\_list\_mng" rowspan="2" class="td\_mng td\_mng\_s"><?php echo $s\_mod ?><?php echo $s\_grp ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 270 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 271 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="mb\_list\_name" class="td\_mbname"><?php echo get\_text($row['mb\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 272 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="mb\_list\_nick" class="td\_name sv\_use"><div><?php echo $mb\_nick ?></div></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 275 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="mb\_sms\_<?php echo $i; ?>" class="sound\_only">SMS수신</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 276 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="mb\_sms[<?php echo $i; ?>]" <?php echo $row['mb\_sms']?'checked':''; ?> value="1" id="mb\_sms\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 279 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="mb\_adult\_<?php echo $i; ?>" class="sound\_only">성인인증</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 280 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="mb\_adult[<?php echo $i; ?>]" <?php echo $row['mb\_adult']?'checked':''; ?> value="1" id="mb\_adult\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 284 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="mb\_intercept\_date[<?php echo $i; ?>]" <?php echo $row['mb\_intercept\_date']?'checked':''; ?> value="<?php echo $intercept\_date ?>" id="mb\_intercept\_date\_<?php echo $i ?>" title="<?php echo $intercept\_title ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 285 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="mb\_intercept\_date\_<?php echo $i; ?>" class="sound\_only">접근차단</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 289 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_level\_select("mb\_level[$i]", 1, $member['mb\_level'], $row['mb\_level']) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 291 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="mb\_list\_tel" class="td\_tel"><?php echo get\_text($row['mb\_tel']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 292 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="mb\_list\_join" class="td\_date"><?php echo substr($row['mb\_datetime'],2,8); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 293 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="mb\_list\_point" class="td\_num"><a href="point\_list.php?sfl=mb\_id&amp;stx=<?php echo $row['mb\_id'] ?>"><?php echo number\_format($row['mb\_point']) ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 300 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<tr><td colspan=\"".$colspan."\" class=\"empty\_table\">자료가 없습니다.</td></tr>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 318 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, '?'.$qstr.'&amp;page='); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\member\_list\_delete.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<script type='text/javascript'> alert('$msg'); </script>";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_form.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$code = isset($\_GET['code']) ? preg\_replace('/[^0-9a-zA-Z]/', '', $\_GET['code']) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title']; ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

add\_menu\_list(me\_name, me\_link, "<?php echo $code; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

add\_menu\_list(me\_name, me\_link, "<?php echo $code; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var list = "<tr class=\"menu\_list menu\_group\_<?php echo $code; ?>\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

list += "<input type=\"hidden\" name=\"code[]\" value=\"<?php echo $code; ?>\">";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_form\_search.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$type = isset($\_REQUEST['type']) ? preg\_replace('/[^0-9a-z\_]/i', '', $\_REQUEST['type']) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_form\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><?php echo $bbs\_subject\_title; ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_form\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $row['subject']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_form\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $group['gr\_subject']; ?></td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_form\_search.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

<input type="hidden" name="subject[]" value="<?php echo preg\_replace('/[\'\"]/', '', $row['subject']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_form\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="subject[]" value="<?php echo preg\_replace('/[\'\"]/', '', $row['subject']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_form\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="link[]" value="<?php echo $link; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_form\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" class="add\_select btn btn\_03"><span class="sound\_only"><?php echo $row['subject']; ?> </span>선택</button>

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['menu\_table']}` (

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?> menu\_list menu\_group\_<?php echo substr($row['me\_code'], 0, 2); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_category<?php echo $sub\_menu\_class; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="code[]" value="<?php echo substr($row['me\_code'], 0, 2) ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="me\_name\_<?php echo $i; ?>" class="sound\_only"><?php echo $sub\_menu\_info; ?> 메뉴<strong class="sound\_only"> 필수</strong></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="me\_link\_<?php echo $i; ?>" class="sound\_only">링크<strong class="sound\_only"> 필수</strong></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="me\_link[]" value="<?php echo $row['me\_link'] ?>" id="me\_link\_<?php echo $i; ?>" required class="required tbl\_input full\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="me\_target\_<?php echo $i; ?>" class="sound\_only">새창</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="me\_target[]" id="me\_target\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="self"<?php echo get\_selected($row['me\_target'], 'self', true); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="blank"<?php echo get\_selected($row['me\_target'], 'blank', true); ?>>사용함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="me\_order\_<?php echo $i; ?>" class="sound\_only">순서</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="me\_order[]" value="<?php echo $row['me\_order'] ?>" id="me\_order\_<?php echo $i; ?>" class="tbl\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="me\_use\_<?php echo $i; ?>" class="sound\_only">PC사용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="me\_use[]" id="me\_use\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"<?php echo get\_selected($row['me\_use'], '1', true); ?>>사용함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0"<?php echo get\_selected($row['me\_use'], '0', true); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="me\_mobile\_use\_<?php echo $i; ?>" class="sound\_only">모바일사용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="me\_mobile\_use[]" id="me\_mobile\_use\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"<?php echo get\_selected($row['me\_mobile\_use'], '1', true); ?>>사용함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0"<?php echo get\_selected($row['me\_mobile\_use'], '0', true); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr id="empty\_menu\_list"><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var list = "<tr id=\"empty\_menu\_list\"><td colspan=\"<?php echo $colspan; ?>\" class=\"empty\_table\">자료가 없습니다.</td></tr>\n";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

if(preg\_match('/^javascript/i', preg\_replace('/[ ]{1,}|[\t]/', '', $\_POST['me\_link'][$i]))){

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\menu\_list\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$\_POST['me\_link'][$i] = is\_array($\_POST['me\_link']) ? clean\_xss\_tags(clean\_xss\_attributes(preg\_replace('/[ ]{2,}|[\t]/', '', $\_POST['me\_link'][$i]), 1)) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$nw\_id = isset($\_REQUEST['nw\_id']) ? preg\_replace('/[^0-9]/', '', $\_REQUEST['nw\_id']) : 0;

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " ALTER TABLE `{$g5['new\_win\_table']}` ADD `nw\_division` VARCHAR(10) NOT NULL DEFAULT 'both' ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="nw\_id" value="<?php echo $nw\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="comm"<?php echo get\_selected($nw['nw\_division'], 'comm'); ?>>커뮤니티</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="both"<?php echo get\_selected($nw['nw\_division'], 'both', true); ?>>커뮤니티와 쇼핑몰</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="shop"<?php echo get\_selected($nw['nw\_division'], 'shop'); ?>>쇼핑몰</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="both"<?php echo get\_selected($nw['nw\_device'], 'both', true); ?>>PC와 모바일</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="pc"<?php echo get\_selected($nw['nw\_device'], 'pc'); ?>>PC</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mobile"<?php echo get\_selected($nw['nw\_device'], 'mobile'); ?>>모바일</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="nw\_disable\_hours" value="<?php echo $nw['nw\_disable\_hours']; ?>" id="nw\_disable\_hours" required class="frm\_input required" size="5"> 시간

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="nw\_begin\_time" value="<?php echo $nw['nw\_begin\_time']; ?>" id="nw\_begin\_time" required class="frm\_input required" size="21" maxlength="19">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="nw\_end\_time" value="<?php echo $nw['nw\_end\_time']; ?>" id="nw\_end\_time" required class="frm\_input required" size="21" maxlength="19">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="nw\_left" value="<?php echo $nw['nw\_left']; ?>" id="nw\_left" required class="frm\_input required" size="5"> px

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="nw\_top" value="<?php echo $nw['nw\_top']; ?>" id="nw\_top" required class="frm\_input required" size="5"> px

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="nw\_width" value="<?php echo $nw['nw\_width'] ?>" id="nw\_width" required class="frm\_input required" size="5"> px

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="nw\_height" value="<?php echo $nw['nw\_height'] ?>" id="nw\_height" required class="frm\_input required" size="5"> px

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo editor\_html('nw\_content', get\_text(html\_purifier($nw['nw\_content']), 0)); ?></td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 5 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$nw\_id = isset($\_REQUEST['nw\_id']) ? preg\_replace('/[^0-9]/', '', $\_REQUEST['nw\_id']) : 0;

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinlist.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE {$g5['g5\_shop\_new\_win\_table']} RENAME TO `{$g5['new\_win\_table']}` ;", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinlist.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$query\_cp = sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['new\_win\_table']}` (

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="local\_ov01 local\_ov"><span class="btn\_ov01"><span class="ov\_txt">전체 </span><span class="ov\_num"> <?php echo $total\_count; ?>건</span></span></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['nw\_id']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><?php echo $row['nw\_subject']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_device"><?php echo $nw\_device; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo substr($row['nw\_begin\_time'],2,14); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo substr($row['nw\_end\_time'],2,14); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['nw\_disable\_hours']; ?>시간</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['nw\_left']; ?>px</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['nw\_top']; ?>px</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['nw\_width']; ?>px</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['nw\_height']; ?>px</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./newwinform.php?w=u&amp;nw\_id=<?php echo $row['nw\_id']; ?>" class="btn btn\_03"><span class="sound\_only"><?php echo $row['nw\_subject']; ?> </span>수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\newwinlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./newwinformupdate.php?w=d&amp;nw\_id=<?php echo $row['nw\_id']; ?>" onclick="return delete\_confirm(this);" class="btn btn\_02"><span class="sound\_only"><?php echo $row['nw\_subject']; ?> </span>삭제</a>

**STANDARD: Potentially Unsafe Code - phpinfo**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\phpinfo.php

This debugging function can expose sensitive data to an attacker. Perform a manual check to ensure that its out put data is not visible to normal users.

phpinfo();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">전체 </span><span class="ov\_num"> <?php echo number\_format($total\_count) ?> 건 </span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '&nbsp;<span class="btn\_ov01"><span class="ov\_txt">' . $mb['mb\_id'] .' 님 포인트 합계 </span><span class="ov\_num"> ' . number\_format($mb['mb\_point']) . '점</span></span>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '&nbsp;<span class="btn\_ov01"><span class="ov\_txt">전체 합계</span><span class="ov\_num">'.number\_format($row2['sum\_point']).'점 </span></span>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mb\_id"<?php echo get\_selected($sfl, "mb\_id"); ?>>회원아이디</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="po\_content"<?php echo get\_selected($sfl, "po\_content"); ?>>내용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx ?>" id="stx" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id[<?php echo $i ?>]" value="<?php echo $row['mb\_id'] ?>" id="mb\_id\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="po\_id[<?php echo $i ?>]" value="<?php echo $row['po\_id'] ?>" id="po\_id\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i; ?>" class="sound\_only"><?php echo $row['po\_content'] ?> 내역</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk[]" value="<?php echo $i ?>" id="chk\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><a href="?sfl=mb\_id&amp;stx=<?php echo $row['mb\_id'] ?>"><?php echo $row['mb\_id'] ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><?php echo get\_text($row2['mb\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left sv\_use"><div><?php echo $mb\_nick ?></div></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><?php echo $link1 ?><?php echo $row['po\_content'] ?><?php echo $link2 ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num td\_pt"><?php echo number\_format($row['po\_point']) ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo $row['po\_datetime'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime2<?php echo $expr; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 160 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

만료<?php echo substr(str\_replace('-', '', $row['po\_expire\_date']), 2); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php } else echo $row['po\_expire\_date'] == '9999-12-31' ? '&nbsp;' : $row['po\_expire\_date']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num td\_pt"><?php echo number\_format($row['po\_mb\_point']) ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 182 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 189 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 190 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 191 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 192 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 193 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo isset($token) ? $token : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 204 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="mb\_id" value="<?php echo $mb\_id ?>" id="mb\_id" class="required frm\_input" required></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 217 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="po\_expire\_term" value="<?php echo $po\_expire\_term; ?>" id="po\_expire\_term" class="frm\_input" size="5"> 일</td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\point\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$expire = isset($\_POST['po\_expire\_term']) ? preg\_replace('/[^0-9]/', '', $\_POST['po\_expire\_term']) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="po\_id" value="<?php echo $po\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><label for="po\_poll<?php echo $i ?>">항목 <?php echo $i ?><?php echo $sound\_only ?></label></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="po\_poll<?php echo $i ?>" value="<?php echo $po\_poll ?>" id="po\_poll<?php echo $i ?>" <?php echo $required ?> class="frm\_input <?php echo $required ?>" maxlength="125">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="po\_cnt<?php echo $i ?>">항목 <?php echo $i ?> 투표수</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="po\_cnt<?php echo $i ?>" value="<?php echo $po\_cnt; ?>" id="po\_cnt<?php echo $i ?>" class="frm\_input" size="3">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="po\_etc" value="<?php echo get\_text($po['po\_etc']) ?>" id="po\_etc" class="frm\_input" size="80" maxlength="125">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_level\_select('po\_level', 1, 10, $po['po\_level']) ?> 이상 투표할 수 있음

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="po\_point" value="<?php echo $po['po\_point'] ?>" id="po\_point" class="frm\_input"> 점

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $po['po\_date']; ?></td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

<td><textarea name="po\_ips" id="po\_ips" readonly rows="10"><?php echo preg\_replace("/\n/", " / ", $po['po\_ips']) ?></textarea></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><textarea name="po\_ips" id="po\_ips" readonly rows="10"><?php echo preg\_replace("/\n/", " / ", $po['po\_ips']) ?></textarea></td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

<td><textarea name="mb\_ids" id="mb\_ids" readonly rows="10"><?php echo preg\_replace("/\n/", " / ", $po['mb\_ids']) ?></textarea></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><textarea name="mb\_ids" id="mb\_ids" readonly rows="10"><?php echo preg\_replace("/\n/", " / ", $po['mb\_ids']) ?></textarea></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./poll\_list.php?<?php echo $qstr ?>" class="btn\_02 btn">목록</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">투표수</span><span class="ov\_num"> <?php echo number\_format($total\_count) ?>개</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="po\_subject"<?php echo get\_selected($sfl, "po\_subject"); ?>>제목</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx ?>" id="stx" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i; ?>" class="sound\_only"><?php echo cut\_str(get\_text($row['po\_subject']),70) ?> 투표</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk[]" value="<?php echo $row['po\_id'] ?>" id="chk\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['po\_id'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><?php echo cut\_str(get\_text($row['po\_subject']),70) ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['po\_level'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row2['sum\_po\_cnt'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_etc"><?php echo $po\_etc ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mng td\_mng\_s"><?php echo $s\_mod ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\poll\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">건수</span><span class="ov\_num"> <?php echo number\_format($total\_count) ?>개</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="pp\_word"<?php echo get\_selected($sfl, "pp\_word"); ?>>검색어</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="pp\_date"<?php echo get\_selected($sfl, "pp\_date"); ?>>등록일</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx ?>" id="stx" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo isset($token) ? $token : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i; ?>" class="sound\_only"><?php echo $word ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk[]" value="<?php echo $row['pp\_id'] ?>" id="chk\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><a href="<?php echo $\_SERVER['SCRIPT\_NAME'] ?>?sfl=pp\_word&amp;stx=<?php echo $word ?>"><?php echo $word ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $row['pp\_date'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $row['pp\_ip'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_rank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_rank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">건수</span><span class="ov\_num"> <?php echo number\_format($total\_count) ?>개</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_rank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="fr\_date" value="<?php echo $fr\_date ?>" id="fr\_date" class="frm\_input" size="11" maxlength="10">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_rank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="to\_date" value="<?php echo $to\_date ?>" id="to\_date" class="frm\_input" size="11" maxlength="10">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_rank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_rank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_rank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_rank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_rank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_rank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo isset($token) ? $token : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_rank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_rank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $rank ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_rank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><?php echo $word ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_rank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['cnt'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_rank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\popular\_rank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page=");

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

if(!sql\_query(" DESCRIBE `{$g5['qa\_config\_table']}` ", false)) {

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['qa\_config\_table']}` (

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['qa\_content\_table']}` (

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " SHOW COLUMNS FROM `{$g5['qa\_content\_table']}` LIKE 'qa\_content' ";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['qa\_content\_table']}` CHANGE `qa\_content` `qa\_content` text NOT NULL ", true);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " insert into `{$g5['qa\_config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['qa\_config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['qa\_config\_table']}`

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_skin\_select('qa', 'qa\_skin', 'qa\_skin', $qaconfig['qa\_skin'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_mobile\_skin\_select('qa', 'qa\_mobile\_skin', 'qa\_mobile\_skin', $qaconfig['qa\_mobile\_skin'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qa\_use\_email" value="1" id="qa\_use\_email" <?php echo $qaconfig['qa\_use\_email']?'checked':''; ?>> <label for="qa\_use\_email">보이기</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qa\_req\_email" value="1" id="qa\_req\_email" <?php echo $qaconfig['qa\_req\_email']?'checked':''; ?>> <label for="qa\_req\_email">필수입력</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 169 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qa\_use\_hp" value="1" id="qa\_use\_hp" <?php echo $qaconfig['qa\_use\_hp']?'checked':''; ?>> <label for="qa\_use\_hp">보이기</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qa\_req\_hp" value="1" id="qa\_req\_hp" <?php echo $qaconfig['qa\_req\_hp']?'checked':''; ?>> <label for="qa\_req\_hp">필수입력</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo option\_selected(0, $qaconfig['qa\_use\_sms'], '사용안함'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo option\_selected(1, $qaconfig['qa\_use\_sms'], '사용함'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 209 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo option\_selected(0, $qaconfig['qa\_use\_editor'], '사용안함'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 210 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo option\_selected(1, $qaconfig['qa\_use\_editor'], '사용함'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 218 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_subject\_len" value="<?php echo $qaconfig['qa\_subject\_len'] ?>" id="qa\_subject\_len" required class="required numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 225 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_mobile\_subject\_len" value="<?php echo $qaconfig['qa\_mobile\_subject\_len'] ?>" id="qa\_mobile\_subject\_len" required class="required numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 231 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_page\_rows" value="<?php echo $qaconfig['qa\_page\_rows'] ?>" id="qa\_page\_rows" required class="required numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 237 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_mobile\_page\_rows" value="<?php echo $qaconfig['qa\_mobile\_page\_rows'] ?>" id="qa\_mobile\_page\_rows" required class="required numeric frm\_input" size="4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 244 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_image\_width" value="<?php echo $qaconfig['qa\_image\_width'] ?>" id="qa\_image\_width" required class="required numeric frm\_input" size="4"> 픽셀

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 251 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

업로드 파일 한개당 <input type="text" name="qa\_upload\_size" value="<?php echo $qaconfig['qa\_upload\_size'] ?>" id="qa\_upload\_size" required class="required numeric frm\_input" size="10"> bytes 이하

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 257 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_include\_head" value="<?php echo $qaconfig['qa\_include\_head'] ?>" id="qa\_include\_head" class="frm\_input" size="50">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 263 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_include\_tail" value="<?php echo $qaconfig['qa\_include\_tail'] ?>" id="qa\_include\_tail" class="frm\_input" size="50">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 275 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $captcha\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 285 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo editor\_html("qa\_content\_head", get\_text(html\_purifier($qaconfig['qa\_content\_head']), 0)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 291 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo editor\_html("qa\_content\_tail", get\_text(html\_purifier($qaconfig['qa\_content\_tail']), 0)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 297 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo editor\_html("qa\_mobile\_content\_head", get\_text(html\_purifier($qaconfig['qa\_mobile\_content\_head']), 0)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 303 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo editor\_html("qa\_mobile\_content\_tail", get\_text(html\_purifier($qaconfig['qa\_mobile\_content\_tail']), 0)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 309 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea id="qa\_insert\_content" name="qa\_insert\_content" rows="5"><?php echo html\_purifier($qaconfig['qa\_insert\_content']); ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 314 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row">여분필드<?php echo $i ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 316 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="qa\_<?php echo $i ?>\_subj">여분필드 <?php echo $i ?> 제목</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 317 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_<?php echo $i ?>\_subj" id="qa\_<?php echo $i ?>\_subj" value="<?php echo get\_text($qaconfig['qa\_'.$i.'\_subj']) ?>" class="frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 318 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="qa\_<?php echo $i ?>">여분필드 <?php echo $i ?> 값</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 319 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_<?php echo $i ?>" value="<?php echo get\_text($qaconfig['qa\_'.$i]) ?>" id="qa\_<?php echo $i ?>" class="frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 352 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var qa\_include\_head = "<?php echo $qaconfig['qa\_include\_head']; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 353 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var qa\_include\_tail = "<?php echo $qaconfig['qa\_include\_tail']; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 390 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo isset($captcha\_js) ? $captcha\_js : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$qa\_include\_head = preg\_replace(array("#[\\\]+$#", "#(<\?php|<\?)#i"), "", substr($qa\_include\_head, 0, 255));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$qa\_include\_tail = preg\_replace(array("#[\\\]+$#", "#(<\?php|<\?)#i"), "", substr($qa\_include\_tail, 0, 255));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\qa\_config\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$qa\_category = preg\_replace("/[\<\>\'\"\\\'\\\"\%\=\(\)\/\^\\*]/", "", $qa\_category);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sendmail\_test.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '다음 '.count($real\_email).'개의 메일 주소로 테스트 메일 발송이 완료되었습니다.';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sendmail\_test.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li>'.$real\_email[$i].'</li>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sendmail\_test.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="email" value="<?php echo $member['mb\_email'] ?>" id="email" required class="required email frm\_input" size="80">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\session\_file\_delete.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list\_tag\_st;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\session\_file\_delete.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li>{$session\_file}</li>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\session\_file\_delete.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list\_tag\_end;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\session\_file\_delete.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="local\_desc01 local\_desc"><p><strong>세션데이터 '.$cnt.'건 삭제 완료됐습니다.</strong><br>프로그램의 실행을 끝마치셔도 좋습니다.</p></div>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">설치된 테마</span><span class="ov\_num"> <?php echo number\_format($total\_count); ?></span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $screenshot; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo get\_text($info['theme\_name']); ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $btn\_active; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./theme\_preview.php?theme=<?php echo $theme[$i]; ?>" class="theme\_pr" target="theme\_preview">미리보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" class="tmli\_dt theme\_preview" data-theme="<?php echo $theme[$i]; ?>">상세보기</button>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme\_config\_load.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$data[$val] = (int)preg\_replace('#[^0-9]#', '', $tconfig[$val]);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme\_detail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $name; ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme\_detail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="theme\_dt\_img"><?php echo $screenshot; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme\_detail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo get\_text($info['detail']); ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme\_detail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($info['version']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme\_detail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $maker; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme\_detail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $license; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme\_detail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./theme\_preview.php?theme=<?php echo $theme; ?>" class="theme\_pr btn\_03" target="theme\_preview">미리보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme\_preview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="./theme\_preview.php?theme=<?php echo $theme.$qstr\_index; ?>">인덱스 화면</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme\_preview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="./theme\_preview.php?theme=<?php echo $theme.$qstr\_list; ?>">게시글 리스트</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme\_preview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="./theme\_preview.php?theme=<?php echo $theme.$qstr\_view; ?>">게시글 보기</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme\_preview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="./theme\_preview.php?theme=<?php echo $theme.$qstr\_shop; ?>">쇼핑몰</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme\_preview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="./theme\_preview.php?theme=<?php echo $theme.$qstr\_ca\_list; ?>">상품리스트</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 160 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme\_preview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="./theme\_preview.php?theme=<?php echo $theme.$qstr\_item; ?>">상품상세</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme\_preview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="./theme\_preview.php?theme=<?php echo $theme.$qstr\_device; ?>"><?php echo (G5\_IS\_MOBILE ? 'PC 버전' : '모바일 버전'); ?></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\theme\_preview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $btn\_active; ?>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\thumbnail\_file\_delete.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$files = glob($dir.'/thumb-\*');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\thumbnail\_file\_delete.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li>'.$thumbnail.'</li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\thumbnail\_file\_delete.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="local\_desc01 local\_desc"><p><strong>썸네일 '.$cnt.'건의 삭제 완료됐습니다.</strong><br>프로그램의 실행을 끝마치셔도 좋습니다.</p></div>'.PHP\_EOL;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 4 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\view.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$call = isset($\_REQUEST['call']) ? strtolower(preg\_replace('/[^a-z0-9\_]/i', '', $\_REQUEST['call'])) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="fr\_date" value="<?php echo $fr\_date ?>" id="fr\_date" class="frm\_input" size="11" maxlength="10">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="to\_date" value="<?php echo $to\_date ?>" id="to\_date" class="frm\_input" size="11" maxlength="10">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="./visit\_list.php<?php echo $query\_string ?>">접속자</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="./visit\_domain.php<?php echo $query\_string ?>">도메인</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="./visit\_browser.php<?php echo $query\_string ?>">브라우저</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="./visit\_os.php<?php echo $query\_string ?>">운영체제</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="./visit\_device.php<?php echo $query\_string ?>">접속기기</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="./visit\_hour.php<?php echo $query\_string ?>">시간</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="./visit\_week.php<?php echo $query\_string ?>">요일</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="./visit\_date.php<?php echo $query\_string ?>">일</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="./visit\_month.php<?php echo $query\_string ?>">월</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="./visit\_year.php<?php echo $query\_string ?>">년</a></li>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_browser.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr\_date = isset($\_REQUEST['fr\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['fr\_date']) : G5\_TIME\_YMD;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_browser.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to\_date = isset($\_REQUEST['to\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['to\_date']) : G5\_TIME\_YMD;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_browser.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_browser.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><strong><?php echo $sum\_count ?></strong></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_browser.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_browser.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $no ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_browser.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_category td\_category1"><?php echo $key ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_browser.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span style="width:<?php echo $s\_rate ?>%"></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_browser.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_c3"><?php echo $count ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_browser.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $s\_rate ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_browser.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_date.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr\_date = isset($\_REQUEST['fr\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['fr\_date']) : G5\_TIME\_YMD;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_date.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to\_date = isset($\_REQUEST['to\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['to\_date']) : G5\_TIME\_YMD;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><strong><?php echo number\_format($sum\_count) ?></strong></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_category"><a href="./visit\_list.php?fr\_date=<?php echo $key ?>&amp;to\_date=<?php echo $key ?>"><?php echo $key ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span style="width:<?php echo $s\_rate ?>%"></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_c3"><?php echo number\_format($value) ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $s\_rate ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_delete.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $year; ?>"><?php echo $year; ?></option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_delete.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $i; ?>"><?php echo $i; ?></option>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_delete\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$year = preg\_replace('/[^0-9]/', '', $\_POST['year']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_delete\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$month = preg\_replace('/[^0-9]/', '', $\_POST['month']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_device.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr\_date = isset($\_REQUEST['fr\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['fr\_date']) : G5\_TIME\_YMD;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_device.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to\_date = isset($\_REQUEST['to\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['to\_date']) : G5\_TIME\_YMD;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_device.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_device.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><strong><?php echo $sum\_count ?></strong></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_device.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_device.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $no ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_device.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_category td\_category1"><?php echo $key ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_device.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span style="width:<?php echo $s\_rate ?>%"></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_device.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_c3"><?php echo $count ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_device.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $s\_rate ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_device.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_domain.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr\_date = isset($\_REQUEST['fr\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['fr\_date']) : G5\_TIME\_YMD;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_domain.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to\_date = isset($\_REQUEST['to\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['to\_date']) : G5\_TIME\_YMD;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_domain.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$s = preg\_replace("/^(www\.|search\.|dirsearch\.|dir\.search\.|dir\.|kr\.search\.|myhome\.)(.\*)/", "\\2", $s);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_domain.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_domain.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><strong><?php echo $sum\_count ?></strong></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_domain.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_domain.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $no ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_domain.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_category"><?php echo $link ?><?php echo $key ?><?php echo $link2 ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_domain.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span style="width:<?php echo $s\_rate ?>%"></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_domain.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_c3"><?php echo $count ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_domain.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $s\_rate ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_domain.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_hour.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr\_date = isset($\_REQUEST['fr\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['fr\_date']) : G5\_TIME\_YMD;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_hour.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to\_date = isset($\_REQUEST['to\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['to\_date']) : G5\_TIME\_YMD;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_hour.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_hour.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><strong><?php echo number\_format($sum\_count) ?></strong></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_hour.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_hour.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_category"><?php echo $hour ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_hour.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span style="width:<?php echo $s\_rate ?>%"></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_hour.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_c3"><?php echo number\_format($count) ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_hour.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $s\_rate ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_hour.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_list.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr\_date = isset($\_REQUEST['fr\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['fr\_date']) : G5\_TIME\_YMD;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_list.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to\_date = isset($\_REQUEST['to\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['to\_date']) : G5\_TIME\_YMD;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_list.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ip = preg\_replace("/([0-9]+).([0-9]+).([0-9]+).([0-9]+)/", G5\_IP\_DISPLAY, $row['vi\_ip']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_category"><?php echo $ip ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $link ?><?php echo $title ?><?php echo $link2 ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_category td\_category1"><?php echo $brow ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_category td\_category3"><?php echo $os ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_category td\_category2"><?php echo $device; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo $row['vi\_date'] ?> <?php echo $row['vi\_time'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없거나 관리자에 의해 삭제되었습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $pagelist;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_month.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr\_date = isset($\_REQUEST['fr\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['fr\_date']) : G5\_TIME\_YMD;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_month.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to\_date = isset($\_REQUEST['to\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['to\_date']) : G5\_TIME\_YMD;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><strong><?php echo number\_format($sum\_count) ?></strong></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_category"><a href="./visit\_date.php?fr\_date=<?php echo $key ?>-01&amp;to\_date=<?php echo $key ?>-31"><?php echo $key ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span style="width:<?php echo $s\_rate ?>%"></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_c3"><?php echo number\_format($value) ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $s\_rate ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_os.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr\_date = isset($\_REQUEST['fr\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['fr\_date']) : G5\_TIME\_YMD;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_os.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to\_date = isset($\_REQUEST['to\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['to\_date']) : G5\_TIME\_YMD;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_os.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_os.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><strong><?php echo $sum\_count ?></strong></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_os.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_os.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $no ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_os.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_category"><?php echo $key ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_os.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span style="width:<?php echo $s\_rate ?>%"></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_os.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_c3"><?php echo $count ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_os.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $s\_rate ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_os.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="vi\_ip"<?php echo get\_selected($sfl, 'vi\_ip'); ?>>IP</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="vi\_referer"<?php echo get\_selected($sfl, 'vi\_referer'); ?>>접속경로</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="vi\_date"<?php echo get\_selected($sfl, 'vi\_date'); ?>>날짜</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" size="20" value="<?php echo stripslashes($stx); ?>" id="sch\_word" class="frm\_input">

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_search.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ip = preg\_replace("/([0-9]+).([0-9]+).([0-9]+).([0-9]+)/", G5\_IP\_DISPLAY, $row['vi\_ip']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_id"><a href="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>?sfl=vi\_ip&amp;stx=<?php echo $ip; ?>"><?php echo $ip; ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><?php echo $link.$title; ?><?php echo $link ? '</a>' : ''; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_idsmall td\_category1"><?php echo $brow; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_idsmall td\_category3"><?php echo $os; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_idsmall td\_category2"><?php echo $device; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><a href="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>?sfl=vi\_date&amp;stx=<?php echo $row['vi\_date']; ?>"><?php echo $row['vi\_date']; ?></a> <?php echo $row['vi\_time']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($i == 0) echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>'; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $pagelist;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_week.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr\_date = isset($\_REQUEST['fr\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['fr\_date']) : G5\_TIME\_YMD;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_week.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to\_date = isset($\_REQUEST['to\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['to\_date']) : G5\_TIME\_YMD;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_week.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_week.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><strong><?php echo $sum\_count ?></strong></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_week.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_week.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_category"><?php echo $weekday[$i] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_week.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span style="width:<?php echo $s\_rate ?>%"></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_week.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_c3"><?php echo $count ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_week.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $s\_rate ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_week.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_year.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr\_date = isset($\_REQUEST['fr\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['fr\_date']) : G5\_TIME\_YMD;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_year.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to\_date = isset($\_REQUEST['to\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['to\_date']) : G5\_TIME\_YMD;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><strong><?php echo number\_format($sum\_count) ?></strong></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_category"><a href="./visit\_month.php?fr\_date=<?php echo $key ?>-01-01&amp;to\_date=<?php echo $key ?>-12-31"><?php echo $key ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span style="width:<?php echo $s\_rate ?>%"></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_c3"><?php echo number\_format($value) ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $s\_rate ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\visit\_year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\write\_count.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<option value=\"{$row['bo\_table']}\"";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\write\_count.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo ">{$row['bo\_subject']}</option>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\write\_count.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<option value=\"{$key}\"";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\write\_count.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo ">{$key}</option>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\write\_count.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="line" <?php echo ($graph == 'line' ? 'selected="selected"' : ''); ?>>선그래프</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\write\_count.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="bar" <?php echo ($graph == 'bar' ? 'selected="selected"' : ''); ?>>막대그래프</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 183 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\write\_count.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var line1 = [<?php echo implode(',', $line1); ?>];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 184 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\write\_count.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var line2 = [<?php echo implode(',', $line2); ?>];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\write\_count.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

label: '<?php echo $day; ?>',

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\\_rewrite\_config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\\_rewrite\_config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input name="cf\_bbs\_rewrite" id="cf\_bbs\_rewrite\_<?php echo $k; ?>" type="radio" value="<?php echo $k; ?>" <?php echo $checked;?> ><label for="cf\_bbs\_rewrite\_<?php echo $k; ?>" class="rules\_label"><?php echo $v['label']; ?></label></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\\_rewrite\_config\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $v['url']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\admin.shop.lib.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $msg;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\ajax.orderitem.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_itname" rowspan="<?php echo $rowspan; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\ajax.orderitem.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./itemform.php?w=u&amp;it\_id=<?php echo $row['it\_id']; ?>"><?php echo $image; ?> <?php echo stripslashes($row['it\_name']); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\ajax.orderitem.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($od['od\_tax\_flag'] && $row['ct\_notax']) echo '[비과세상품]'; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\ajax.orderitem.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $opt['ct\_option']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\ajax.orderitem.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mngsmall"><?php echo $opt['ct\_status']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\ajax.orderitem.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_cntsmall"><?php echo $opt['ct\_qty']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\ajax.orderitem.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($opt\_price); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\ajax.orderitem.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($ct\_price['stotal']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\ajax.orderitem.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($opt['cp\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\ajax.orderitem.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($ct\_point['stotal']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\ajax.orderitem.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_sendcost\_by"><?php echo $ct\_send\_cost; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\ajax.skinfile.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_list\_skin\_options("^list.[0-9]+\.skin\.php", $skin\_dir, $sval);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$bn\_id = isset($\_REQUEST['bn\_id']) ? preg\_replace('/[^0-9]/', '', $\_REQUEST['bn\_id']) : 0;

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_banner\_table']}`

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bn\_id" value="<?php echo $bn\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $bimg\_str;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bn\_alt" value="<?php echo get\_text($bn['bn\_alt']); ?>" id="bn\_alt" class="frm\_input" size="80">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="both"<?php echo get\_selected($bn['bn\_device'], 'both', true); ?>>PC와 모바일</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="pc"<?php echo get\_selected($bn['bn\_device'], 'pc'); ?>>PC</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mobile"<?php echo get\_selected($bn['bn\_device'], 'mobile'); ?>>모바일</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="왼쪽" <?php echo get\_selected($bn['bn\_position'], '왼쪽'); ?>>왼쪽</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="메인" <?php echo get\_selected($bn['bn\_position'], '메인'); ?>>메인</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected($bn['bn\_border'], 0); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($bn['bn\_border'], 1); ?>>사용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected($bn['bn\_new\_win'], 0); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($bn['bn\_new\_win'], 1); ?>>사용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bn\_begin\_time" value="<?php echo $bn['bn\_begin\_time']; ?>" id="bn\_begin\_time" class="frm\_input" size="21" maxlength="19">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bn\_end\_time" value="<?php echo $bn['bn\_end\_time']; ?>" id="bn\_end\_time" class="frm\_input" size=21 maxlength=19>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo order\_select("bn\_order", $bn['bn\_order']); ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$bn\_id = isset($\_REQUEST['bn\_id']) ? preg\_replace('/[^0-9]/', '', $\_REQUEST['bn\_id']) : 0;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$bn\_bimg\_del = (isset($\_POST['bn\_bimg\_del']) && $\_POST['bn\_bimg\_del']) ? preg\_replace('/[^0-9]/', '', $\_POST['bn\_id']) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt"> <?php echo ($sql\_search) ? '검색' : '등록'; ?>된 배너 </span><span class="ov\_num"> <?php echo $total\_count; ?>개</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value=""<?php echo get\_selected($bn\_position, '', true); ?>>위치 전체</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="메인"<?php echo get\_selected($bn\_position, '메인', true); ?>>메인</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="왼쪽"<?php echo get\_selected($bn\_position, '왼쪽', true); ?>>왼쪽</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="both"<?php echo get\_selected($bn\_device, 'both', true); ?>>PC와 모바일</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="pc"<?php echo get\_selected($bn\_device, 'pc'); ?>>PC</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mobile"<?php echo get\_selected($bn\_device, 'mobile'); ?>>모바일</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value=""<?php echo get\_selected($bn\_time, '', true); ?>>배너 시간 전체</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="ing"<?php echo get\_selected($bn\_time, 'ing'); ?>>진행중인 배너</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="end"<?php echo get\_selected($bn\_time, 'end'); ?>>종료된 배너</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$bn\_img .= '<img src="'.G5\_DATA\_URL.'/banner/'.$row['bn\_id'].'?'.preg\_replace('/[^0-9]/i', '', $row['bn\_time']).'" width="'.$width.'" alt="'.get\_text($row['bn\_alt']).'">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_id" rowspan="2" class="td\_num"><?php echo $row['bn\_id']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_dvc"><?php echo $bn\_device; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_loc"><?php echo $row['bn\_position']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_st" class="td\_datetime"><?php echo $bn\_begin\_time; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_end" class="td\_datetime"><?php echo $bn\_end\_time; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_odr" class="td\_num"><?php echo $row['bn\_order']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_hit" class="td\_num"><?php echo $row['bn\_hit']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./bannerform.php?w=u&amp;bn\_id=<?php echo $row['bn\_id']; ?>" class="btn btn\_03">수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./bannerformupdate.php?w=d&amp;bn\_id=<?php echo $row['bn\_id']; ?>" onclick="return delete\_confirm(this);" class="btn btn\_02">삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 160 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sbn\_image"><?php echo $bn\_img; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\bannerlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ca\_id = isset($\_GET['ca\_id']) ? preg\_replace('/[^0-9a-z]/i', '', $\_GET['ca\_id']) : '';

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_category\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_category\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_category\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_category\_table']}` ADD INDEX(`ca\_order`) ", true);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_category\_table']}`

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 160 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ca\_explan\_html" value="<?php echo $ca['ca\_explan\_html']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 185 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_id" value="<?php echo $subid; ?>" id="ca\_id" required class="required frm\_input" size="<?php echo $sublen; ?>" maxlength="<?php echo $sublen; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ca\_id" value="<?php echo $ca['ca\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="frm\_ca\_id"><?php echo $ca['ca\_id']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 189 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo shop\_category\_url($ca\_id); ?>" class="btn\_frmline">미리보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 190 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./categoryform.php?ca\_id=<?php echo $ca\_id; ?>&amp;<?php echo $qstr; ?>" class="btn\_frmline">하위분류 추가</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 191 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./itemlist.php?sca=<?php echo $ca['ca\_id']; ?>" class="btn\_frmline">상품리스트</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 197 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="ca\_name" value="<?php echo $ca['ca\_name']; ?>" id="ca\_name" size="38" required class="required frm\_input"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 203 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_order" value="<?php echo $ca['ca\_order']; ?>" id="ca\_order" class="frm\_input" size="12">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 213 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $ca['ca\_mb\_id']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 220 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_skin\_select('shop', 'ca\_skin\_dir', 'ca\_skin\_dir', $ca['ca\_skin\_dir']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 226 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_mobile\_skin\_select('shop', 'ca\_mobile\_skin\_dir', 'ca\_mobile\_skin\_dir', $ca['ca\_mobile\_skin\_dir']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 232 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="ca\_cert\_use" value="1" id="ca\_cert\_use\_yes" <?php if($ca['ca\_cert\_use']) echo 'checked="checked"'; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 234 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="ca\_cert\_use" value="0" id="ca\_cert\_use\_no" <?php if(!$ca['ca\_cert\_use']) echo 'checked="checked"'; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 241 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="ca\_adult\_use" value="1" id="ca\_adult\_use\_yes" <?php if($ca['ca\_adult\_use']) echo 'checked="checked"'; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 243 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="ca\_adult\_use" value="0" id="ca\_adult\_use\_no" <?php if(!$ca['ca\_adult\_use']) echo 'checked="checked"'; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 250 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo help('기본으로 제공하는 스킨은 '.str\_replace(G5\_PATH.'/', '', $g5\_shop\_skin\_path).'/list.\*.skin.php 입니다.'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 252 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^list.[0-9]+\.skin\.php", $g5\_shop\_skin\_path, $ca['ca\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 260 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_img\_width" value="<?php echo $ca['ca\_img\_width']; ?>" id="ca\_img\_width" required class="required frm\_input" size="5" > 픽셀

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 267 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_img\_height" value="<?php echo $ca['ca\_img\_height']; ?>" id="ca\_img\_height" required class="required frm\_input" size="5" > 픽셀

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 274 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_list\_mod" size="3" value="<?php echo $ca['ca\_list\_mod']; ?>" id="ca\_list\_mod" required class="required frm\_input"> 개

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 281 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_list\_row" value='<?php echo $ca['ca\_list\_row']; ?>' id="ca\_list\_row" required class="required frm\_input" size="3"> 줄

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 287 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo help('기본으로 제공하는 스킨은 '.str\_replace(G5\_PATH.'/', '', $g5\_mshop\_skin\_path).'/list.\*.skin.php 입니다.'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 289 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^list.[0-9]+\.skin\.php", $g5\_mshop\_skin\_path, $ca['ca\_mobile\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 297 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_mobile\_img\_width" value="<?php echo $ca['ca\_mobile\_img\_width']; ?>" id="ca\_mobile\_img\_width" required class="required frm\_input" size="5" > 픽셀

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 304 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_mobile\_img\_height" value="<?php echo $ca['ca\_mobile\_img\_height']; ?>" id="ca\_mobile\_img\_height" required class="required frm\_input" size="5" > 픽셀

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 311 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_mobile\_list\_mod" value='<?php echo $ca['ca\_mobile\_list\_mod']; ?>' id="ca\_mobile\_list\_mod" required class="required frm\_input" size="3"> 개

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 318 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_mobile\_list\_row" value='<?php echo $ca['ca\_mobile\_list\_row']; ?>' id="ca\_mobile\_list\_row" required class="required frm\_input" size="3"> 줄

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 325 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_stock\_qty" size="10" value="<?php echo $ca['ca\_stock\_qty']; ?>" id="ca\_stock\_qty" class="frm\_input"> 개

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 339 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="ca\_use" <?php echo ($ca['ca\_use']) ? "checked" : ""; ?> value="1" id="ca\_use">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 347 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="ca\_nocoupon" <?php echo ($ca['ca\_nocoupon']) ? "checked" : ""; ?> value="1" id="ca\_nocoupon">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 360 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 374 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_include\_head" value="<?php echo $ca['ca\_include\_head']; ?>" id="ca\_include\_head" class="frm\_input" size="60">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 381 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_include\_tail" value="<?php echo $ca['ca\_include\_tail']; ?>" id="ca\_include\_tail" class="frm\_input" size="60">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 393 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $captcha\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 404 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo editor\_html('ca\_head\_html', get\_text(html\_purifier($ca['ca\_head\_html']), 0)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 411 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo editor\_html('ca\_tail\_html', get\_text(html\_purifier($ca['ca\_tail\_html']), 0)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 418 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo editor\_html('ca\_mobile\_head\_html', get\_text(html\_purifier($ca['ca\_mobile\_head\_html']), 0)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 425 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo editor\_html('ca\_mobile\_tail\_html', get\_text(html\_purifier($ca['ca\_mobile\_tail\_html']), 0)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 436 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 447 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row">여분필드<?php echo $i ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 449 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_<?php echo $i ?>\_subj">여분필드 <?php echo $i ?> 제목</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 450 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_<?php echo $i ?>\_subj" id="ca\_<?php echo $i ?>\_subj" value="<?php echo get\_text($ca['ca\_'.$i.'\_subj']) ?>" class="frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 451 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_<?php echo $i ?>">여분필드 <?php echo $i ?> 값</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 452 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_<?php echo $i ?>" value="<?php echo get\_text($ca['ca\_'.$i]) ?>" id="ca\_<?php echo $i ?>" class="frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 465 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 491 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./categorylist.php?<?php echo $qstr; ?>" class="btn\_02 btn">목록</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 579 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var ca\_include\_head = "<?php echo $ca['ca\_include\_head']; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 580 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var ca\_include\_tail = "<?php echo $ca['ca\_include\_tail']; ?>";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categoryformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ca\_id = isset($\_REQUEST['ca\_id']) ? preg\_replace('/[^0-9a-z]/i', '', $\_REQUEST['ca\_id']) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">생성된 분류 수</span><span class="ov\_num"> <?php echo number\_format($total\_count); ?>개</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="save\_stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="ca\_name"<?php echo get\_selected($sfl, "ca\_name", true); ?>>분류명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="ca\_id"<?php echo get\_selected($sfl, "ca\_id", true); ?>>분류코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="ca\_mb\_id"<?php echo get\_selected($sfl, "ca\_mb\_id", true); ?>>회원아이디</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx; ?>" id="stx" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ca\_id[<?php echo $i; ?>]" value="<?php echo $row['ca\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo shop\_category\_url($row['ca\_id']); ?>"><?php echo $row['ca\_id']; ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="sct\_cate" class="sct\_name<?php echo $level; ?>"><?php echo $s\_level; ?> <input type="text" name="ca\_name[<?php echo $i; ?>]" value="<?php echo get\_text($row['ca\_name']); ?>" id="ca\_name\_<?php echo $i; ?>" required class="tbl\_input full\_input required"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 174 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="sct\_amount" class="td\_amount"><a href="./itemlist.php?sca=<?php echo $row['ca\_id']; ?>"><?php echo $row1['cnt']; ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="ca\_cert\_use[<?php echo $i; ?>]" value="1" id="ca\_cert\_use\_yes<?php echo $i; ?>" <?php if($row['ca\_cert\_use']) echo 'checked="checked"'; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_cert\_use\_yes<?php echo $i; ?>">사용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_out\_width<?php echo $i; ?>" class="sound\_only">출력이미지 폭</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 181 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_img\_width[<?php echo $i; ?>]" value="<?php echo get\_text($row['ca\_img\_width']); ?>" id="ca\_out\_width<?php echo $i; ?>" required class="required tbl\_input" size="3" > <span class="sound\_only">픽셀</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 185 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_lineimg\_num<?php echo $i; ?>" class="sound\_only">1줄당 이미지 수</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 186 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_list\_mod[<?php echo $i; ?>]" size="3" value="<?php echo $row['ca\_list\_mod']; ?>" id="ca\_lineimg\_num<?php echo $i; ?>" required class="required tbl\_input"> <span class="sound\_only">개</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 189 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_mobileimg\_num<?php echo $i; ?>" class="sound\_only">모바일 1줄당 이미지 수</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 190 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_mobile\_list\_mod[<?php echo $i; ?>]" size="3" value="<?php echo $row['ca\_mobile\_list\_mod']; ?>" id="ca\_mobileimg\_num<?php echo $i; ?>" required class="required tbl\_input"> <span class="sound\_only">개</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 193 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_skin\_dir<?php echo $i; ?>" class="sound\_only">PC스킨폴더</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 194 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_skin\_select('shop', 'ca\_skin\_dir'.$i, 'ca\_skin\_dir['.$i.']', $row['ca\_skin\_dir'], 'class="skin\_dir"'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_skin<?php echo $i; ?>" class="sound\_only">PC스킨파일</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 196 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select id="ca\_skin<?php echo $i; ?>" name="ca\_skin[<?php echo $i; ?>]" required class="required">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 197 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^list.[0-9]+\.skin\.php", $g5\_shop\_skin\_path, $row['ca\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 201 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $s\_add; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 202 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $s\_vie; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 203 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $s\_upd; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 204 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $s\_del; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 207 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 210 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_mb\_id<?php echo $i; ?>" class="sound\_only">관리회원아이디</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 211 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_mb\_id[<?php echo $i; ?>]" value="<?php echo $row['ca\_mb\_id']; ?>" id="ca\_mb\_id<?php echo $i; ?>" class="tbl\_input full\_input" size="15" maxlength="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 213 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ca\_mb\_id[<?php echo $i; ?>]" value="<?php echo $row['ca\_mb\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 214 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $row['ca\_mb\_id']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 218 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="ca\_use[<?php echo $i; ?>]" value="1" id="ca\_use<?php echo $i; ?>" <?php echo ($row['ca\_use'] ? "checked" : ""); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 219 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_use<?php echo $i; ?>">판매</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 223 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="ca\_adult\_use[<?php echo $i; ?>]" value="1" id="ca\_adult\_use\_yes<?php echo $i; ?>" <?php if($row['ca\_adult\_use']) echo 'checked="checked"'; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 224 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_adult\_use\_yes<?php echo $i; ?>">사용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 227 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_img\_height<?php echo $i; ?>" class="sound\_only">출력이미지 높이</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 228 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_img\_height[<?php echo $i; ?>]" value="<?php echo $row['ca\_img\_height']; ?>" id="ca\_img\_height<?php echo $i; ?>" required class="required tbl\_input" size="3" > <span class="sound\_only">픽셀</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 231 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_imgline\_num<?php echo $i; ?>" class="sound\_only">이미지 줄 수</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 232 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_list\_row[<?php echo $i; ?>]" value='<?php echo $row['ca\_list\_row']; ?>' id="ca\_imgline\_num<?php echo $i; ?>" required class="required tbl\_input" size="3"> <span class="sound\_only">줄</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 235 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_mobileimg\_row<?php echo $i; ?>" class="sound\_only">모바일 이미지 줄 수</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ca\_mobile\_list\_row[<?php echo $i; ?>]" value='<?php echo $row['ca\_mobile\_list\_row']; ?>' id="ca\_mobileimg\_row<?php echo $i; ?>" required class="required tbl\_input" size="3">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 239 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_mobile\_skin\_dir<?php echo $i; ?>" class="sound\_only">모바일스킨폴더</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 240 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_mobile\_skin\_select('shop', 'ca\_mobile\_skin\_dir'.$i, 'ca\_mobile\_skin\_dir['.$i.']', $row['ca\_mobile\_skin\_dir'], 'class="skin\_dir"'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 241 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_mobile\_skin<?php echo $i; ?>" class="sound\_only">모바일스킨파일</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 242 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select id="ca\_mobile\_skin<?php echo $i; ?>" name="ca\_mobile\_skin[<?php echo $i; ?>]" required class="required">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 243 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^list.[0-9]+\.skin\.php", $g5\_mshop\_skin\_path, $row['ca\_mobile\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 248 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo "<tr><td colspan=\"9\" class=\"empty\_table\">자료가 한 건도 없습니다.</td></tr>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 264 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\categorylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['g5\_shop\_post\_log\_table']}` (

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 193 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = "ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 200 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = "ALTER TABLE `{$g5['g5\_shop\_default\_table']}`

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 218 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 300 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 316 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_skin\_select('shop', 'de\_shop\_skin', 'de\_shop\_skin', $default['de\_shop\_skin'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 322 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_mobile\_skin\_select('shop', 'de\_shop\_mobile\_skin', 'de\_shop\_mobile\_skin', $default['de\_shop\_mobile\_skin'], 'required'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 334 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 354 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_type1\_list\_use" value="1" id="de\_type1\_list\_use" <?php echo $default['de\_type1\_list\_use']?"checked":""; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 357 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^main.[0-9]+\.skin\.php", G5\_SHOP\_SKIN\_PATH, $default['de\_type1\_list\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 373 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_type2\_list\_use" value="1" id="de\_type2\_list\_use" <?php echo $default['de\_type2\_list\_use']?"checked":""; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 376 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^main.[0-9]+\.skin\.php", G5\_SHOP\_SKIN\_PATH, $default['de\_type2\_list\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 392 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_type3\_list\_use" value="1" id="de\_type3\_list\_use" <?php echo $default['de\_type3\_list\_use']?"checked":""; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 395 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^main.[0-9]+\.skin\.php", G5\_SHOP\_SKIN\_PATH, $default['de\_type3\_list\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 411 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_type4\_list\_use" value="1" id="de\_type4\_list\_use" <?php echo $default['de\_type4\_list\_use']?"checked":""; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 414 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^main.[0-9]+\.skin\.php", G5\_SHOP\_SKIN\_PATH, $default['de\_type4\_list\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 430 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_type5\_list\_use" value="1" id="de\_type5\_list\_use" <?php echo $default['de\_type5\_list\_use']?"checked":""; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 433 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^main.[0-9]+\.skin\.php", G5\_SHOP\_SKIN\_PATH, $default['de\_type5\_list\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 454 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 474 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_mobile\_type1\_list\_use" value="1" id="de\_mobile\_type1\_list\_use" <?php echo $default['de\_mobile\_type1\_list\_use']?"checked":""; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 477 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^main.[0-9]+\.skin\.php", G5\_MSHOP\_SKIN\_PATH, $default['de\_mobile\_type1\_list\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 492 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="de\_mobile\_type2\_list\_use">출력</label> <input type="checkbox" name="de\_mobile\_type2\_list\_use" value="1" id="de\_mobile\_type2\_list\_use" <?php echo $default['de\_mobile\_type2\_list\_use']?"checked":""; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 495 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^main.[0-9]+\.skin\.php", G5\_MSHOP\_SKIN\_PATH, $default['de\_mobile\_type2\_list\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 511 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_mobile\_type3\_list\_use" value="1" id="de\_mobile\_type3\_list\_use" <?php echo $default['de\_mobile\_type3\_list\_use']?"checked":""; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 514 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^main.[0-9]+\.skin\.php", G5\_MSHOP\_SKIN\_PATH, $default['de\_mobile\_type3\_list\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 530 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_mobile\_type4\_list\_use" value="1" id="de\_mobile\_type4\_list\_use" <?php echo $default['de\_mobile\_type4\_list\_use']?"checked":""; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 533 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^main.[0-9]+\.skin\.php", G5\_MSHOP\_SKIN\_PATH, $default['de\_mobile\_type4\_list\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 549 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_mobile\_type5\_list\_use" value="1" id="de\_mobile\_type5\_list\_use" <?php echo $default['de\_mobile\_type5\_list\_use']?"checked":""; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 552 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^main.[0-9]+\.skin\.php", G5\_MSHOP\_SKIN\_PATH, $default['de\_mobile\_type5\_list\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 573 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 588 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected($default['de\_bank\_use'], 0); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 589 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($default['de\_bank\_use'], 1); ?>>사용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 596 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="de\_bank\_account" id="de\_bank\_account"><?php echo $default['de\_bank\_account']; ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 604 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected($default['de\_iche\_use'], 0); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 605 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($default['de\_iche\_use'], 1); ?>>사용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 614 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected($default['de\_vbank\_use'], 0); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 615 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($default['de\_vbank\_use'], 1); ?>>사용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 636 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected($default['de\_hp\_use'], 0); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 637 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($default['de\_hp\_use'], 1); ?>>사용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 646 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected($default['de\_card\_use'], 0); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 647 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($default['de\_card\_use'], 1); ?>>사용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 656 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected($default['de\_card\_noint\_use'], 0); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 657 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($default['de\_card\_noint\_use'], 1); ?>>사용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 666 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected($default['de\_easy\_pay\_use'], 0); ?>>노출안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 667 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($default['de\_easy\_pay\_use'], 1); ?>>노출함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 676 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected($default['de\_taxsave\_use'], 0); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 677 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($default['de\_taxsave\_use'], 1); ?>>사용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 698 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="de\_taxsave\_types\_account" name="de\_taxsave\_types\_account" value="account" <?php echo $account\_checked; ?> > <label for="de\_taxsave\_types\_account" disabled>무통장입금</label><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 699 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="de\_taxsave\_types\_vbank" name="de\_taxsave\_types\_vbank" value="vbank" <?php echo $vbank\_checked; ?> > <label for="de\_taxsave\_types\_vbank">가상계좌</label><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 700 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="de\_taxsave\_types\_transfer" name="de\_taxsave\_types\_transfer" value="transfer" <?php echo $transfer\_checked; ?> > <label for="de\_taxsave\_types\_transfer">실시간계좌이체</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 707 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="cf\_use\_point" value="1" id="cf\_use\_point"<?php echo $config['cf\_use\_point']?' checked':''; ?>> 사용

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 729 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="100" <?php echo get\_selected($default['de\_settle\_point\_unit'], 100); ?>>100</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 730 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="10" <?php echo get\_selected($default['de\_settle\_point\_unit'], 10); ?>>10</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 731 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($default['de\_settle\_point\_unit'], 1); ?>>1</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 740 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected($default['de\_card\_point'], 0); ?>>아니오</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 741 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($default['de\_card\_point'], 1); ?>>예</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 755 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="de\_pg\_service" id="de\_pg\_service" value="<?php echo $default['de\_pg\_service']; ?>" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 758 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php if($default['de\_pg\_service'] == 'kcp') echo 'tab-current'; ?>"><a href="#kcp\_info\_anchor" data-value="kcp" title="NHN KCP 선택하기" >NHN KCP</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 759 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php if($default['de\_pg\_service'] == 'lg') echo 'tab-current'; ?>"><a href="#lg\_info\_anchor" data-value="lg" title="토스페이먼츠 선택하기">토스페이먼츠</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 760 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php if($default['de\_pg\_service'] == 'inicis') echo 'tab-current'; ?>"><a href="#inicis\_info\_anchor" data-value="inicis" title="KG이니시스 선택하기">KG이니시스</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 785 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="de\_easy\_nhnkcp\_payco" name="de\_easy\_pays[]" value="nhnkcp\_payco" <?php if(stripos($default['de\_easy\_pay\_services'], 'nhnkcp\_payco') !== false){ echo 'checked="checked"'; } ?> > <label for="de\_easy\_nhnkcp\_payco" disabled>PAYCO (페이코)</label><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 786 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="de\_easy\_nhnkcp\_naverpay" name="de\_easy\_pays[]" value="nhnkcp\_naverpay" <?php if(stripos($default['de\_easy\_pay\_services'], 'nhnkcp\_naverpay') !== false){ echo 'checked="checked"'; } ?> > <label for="de\_easy\_nhnkcp\_naverpay">NAVERPAY (네이버페이)</label><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 787 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="de\_easy\_nhnkcp\_kakaopay" name="de\_easy\_pays[]" value="nhnkcp\_kakaopay" <?php if(stripos($default['de\_easy\_pay\_services'], 'nhnkcp\_kakaopay') !== false){ echo 'checked="checked"'; } ?> > <label for="de\_easy\_nhnkcp\_kakaopay">KAKAOPAY (카카오페이)</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 794 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="de\_global\_nhnkcp\_naverpay" name="de\_easy\_pays[]" value="global\_nhnkcp\_naverpay" <?php if(stripos($default['de\_easy\_pay\_services'], 'global\_nhnkcp\_naverpay') !== false){ echo 'checked="checked"'; } ?> > <label for="de\_global\_nhnkcp\_naverpay">NAVERPAY (네이버페이)</label><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 801 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="used\_nhnkcp\_naverpay\_point" name="de\_easy\_pays[]" value="used\_nhnkcp\_naverpay\_point" <?php if(stripos($default['de\_easy\_pay\_services'], 'used\_nhnkcp\_naverpay\_point') !== false){ echo 'checked="checked"'; } ?> > <label for="used\_nhnkcp\_naverpay\_point">NAVERPAY POINT (네이버페이 포인트 사용)</label><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 828 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sitecode">SIR</span> <input type="text" name="de\_inicis\_mid" value="<?php echo $default['de\_inicis\_mid']; ?>" id="de\_inicis\_mid" class="frm\_input code\_input" size="10" maxlength="10"> 영문소문자(숫자포함 가능)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 852 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_samsung\_pay\_use" value="1" id="de\_samsung\_pay\_use"<?php echo $default['de\_samsung\_pay\_use']?' checked':''; ?>> <label for="de\_samsung\_pay\_use">사용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 861 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_inicis\_lpay\_use" value="1" id="de\_inicis\_lpay\_use"<?php echo $default['de\_inicis\_lpay\_use']?' checked':''; ?>> <label for="de\_inicis\_lpay\_use">사용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 870 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_inicis\_kakaopay\_use" value="1" id="de\_inicis\_kakaopay\_use"<?php echo $default['de\_inicis\_kakaopay\_use']?' checked':''; ?>> <label for="de\_inicis\_kakaopay\_use">사용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 879 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_inicis\_cartpoint\_use" value="1" id="de\_inicis\_cartpoint\_use"<?php echo $default['de\_inicis\_cartpoint\_use']?' checked':''; ?>> <label for="de\_inicis\_cartpoint\_use">사용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 912 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_kakaopay\_enckey" value="1" id="de\_kakaopay\_enckey"<?php echo $default['de\_kakaopay\_enckey']?' checked':''; ?>> <label for="de\_kakaopay\_enckey">사용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 956 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($default['de\_naverpay\_test'], 1); ?>>예</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 957 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected($default['de\_naverpay\_test'], 0); ?>>아니오</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 991 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="de\_escrow\_use" value="0" <?php echo $default['de\_escrow\_use']==0?"checked":""; ?> id="de\_escrow\_use1">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 993 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="de\_escrow\_use" value="1" <?php echo $default['de\_escrow\_use']==1?"checked":""; ?> id="de\_escrow\_use2">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1001 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="de\_card\_test" value="0" <?php echo $default['de\_card\_test']==0?"checked":""; ?> id="de\_card\_test1">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1003 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="de\_card\_test" value="1" <?php echo $default['de\_card\_test']==1?"checked":""; ?> id="de\_card\_test2">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1048 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_tax\_flag\_use" value="1" id="de\_tax\_flag\_use"<?php echo $default['de\_tax\_flag\_use']?' checked':''; ?>> 사용

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1058 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$(".<?php echo $default['de\_pg\_service']; ?>\_cardtest").removeClass("scf\_cardtest\_hide");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1059 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$("#<?php echo $default['de\_pg\_service']; ?>\_cardtest\_tip").removeClass("scf\_cardtest\_tip\_adm\_hide");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1067 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1082 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_delivery\_company($default['de\_delivery\_company']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1091 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="차등" <?php echo get\_selected($default['de\_send\_cost\_case'], "차등"); ?>>금액별차등</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1092 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="무료" <?php echo get\_selected($default['de\_send\_cost\_case'], "무료"); ?>>무료배송</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected($default['de\_hope\_date\_use'], 0); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($default['de\_hope\_date\_use'], 1); ?>>사용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo editor\_html('de\_baesong\_content', get\_text(html\_purifier($default['de\_baesong\_content']), 0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo editor\_html('de\_change\_content', get\_text(html\_purifier($default['de\_change\_content']), 0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^relation.[0-9]+\.skin\.php", G5\_SHOP\_SKIN\_PATH, $default['de\_rel\_list\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_rel\_list\_use" value="1" id="de\_rel\_list\_use" <?php echo $default['de\_rel\_list\_use']?"checked":""; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^relation.[0-9]+\.skin\.php", G5\_MSHOP\_SKIN\_PATH, $default['de\_mobile\_rel\_list\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1185 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_mobile\_rel\_list\_use" value="1" id="de\_mobile\_rel\_list\_use" <?php echo $default['de\_mobile\_rel\_list\_use']?"checked":""; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1193 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^list.[0-9]+\.skin\.php", G5\_SHOP\_SKIN\_PATH, $default['de\_search\_list\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1210 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^list.[0-9]+\.skin\.php", G5\_MSHOP\_SKIN\_PATH, $default['de\_mobile\_search\_list\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1227 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^list.[0-9]+\.skin\.php", G5\_SHOP\_SKIN\_PATH, $default['de\_listtype\_list\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1244 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^list.[0-9]+\.skin\.php", G5\_MSHOP\_SKIN\_PATH, $default['de\_mobile\_listtype\_list\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1379 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected($default['de\_item\_use\_write'], 0); ?>>주문상태와 무관하게 작성가능</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1380 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($default['de\_item\_use\_write'], 1); ?>>주문상태가 완료인 경우에만 작성가능</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1389 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected($default['de\_item\_use\_use'], 0); ?>>즉시 출력</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1390 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($default['de\_item\_use\_use'], 1); ?>>관리자 승인 후 출력</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1398 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_level\_select('de\_level\_sell', 1, 10, $default['de\_level\_sell']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1412 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_guest\_cart\_use" value="1" id="de\_guest\_cart\_use"<?php echo $default['de\_guest\_cart\_use']?' checked':''; ?>> 사용

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1420 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_member\_reg\_coupon\_use" value="1" id="de\_member\_reg\_coupon\_use"<?php echo $default['de\_member\_reg\_coupon\_use']?' checked':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1431 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo editor\_html('de\_guest\_privacy', get\_text(html\_purifier($default['de\_guest\_privacy']), 0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1443 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo ($\_SERVER['SERVER\_ADDR']?$\_SERVER['SERVER\_ADDR']:$\_SERVER['LOCAL\_ADDR']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1549 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1564 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="" <?php echo get\_selected($config['cf\_sms\_use'], ''); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1565 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="icode" <?php echo get\_selected($config['cf\_sms\_use'], 'icode'); ?>>아이코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1574 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="" <?php echo get\_selected($config['cf\_sms\_type'], ''); ?>>SMS</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1575 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="LMS" <?php echo get\_selected($config['cf\_sms\_type'], 'LMS'); ?>>LMS</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1600 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="icode\_old\_version <?php if(!(isset($userinfo['payment']) && $userinfo['payment'])){ echo 'cf\_tr\_hide'; } ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1622 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo number\_format($userinfo['coin']); ?> 원.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1623 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="http://www.icodekorea.com/smsbiz/credit\_card\_amt.php?icode\_id=<?php echo $config['cf\_icode\_id']; ?>&amp;icode\_passwd=<?php echo $config['cf\_icode\_pw']; ?>" target="\_blank" class="btn\_frmline" onclick="window.open(this.href,'icode\_payment', 'scrollbars=1,resizable=1'); return false;">충전하기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1634 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

서버아이피 : <?php echo $\_SERVER['SERVER\_ADDR']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1670 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h4><?php echo $scf\_sms\_title[$i]; ?></h4>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1671 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="de\_sms\_use<?php echo $i; ?>" value="1" id="de\_sms\_use<?php echo $i; ?>" <?php echo ($default["de\_sms\_use".$i] ? " checked" : ""); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1672 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="de\_sms\_use<?php echo $i; ?>"><span class="sound\_only"><?php echo $scf\_sms\_title[$i]; ?></span>사용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1674 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea id="de\_sms\_cont<?php echo $i; ?>" name="de\_sms\_cont<?php echo $i; ?>" ONKEYUP="byte\_check('de\_sms\_cont<?php echo $i; ?>', 'byte<?php echo $i; ?>');"><?php echo html\_purifier($default['de\_sms\_cont'.$i]); ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1676 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="byte<?php echo $i; ?>" class="scf\_sms\_cnt">0 / 80 바이트</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1680 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

byte\_check('de\_sms\_cont<?php echo $i; ?>', 'byte<?php echo $i; ?>');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1774 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$("#<?php echo $default['de\_pg\_service']; ?>\_vbank\_url").show();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1936 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo module\_exec\_check(G5\_SHOP\_PATH.$exe, 'pp\_cli');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1979 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'alert("'.str\_replace(G5\_PATH.'/', '',$log\_path).' 폴더에 쓰기권한을 부여해 주십시오.\n> chmod 707 log");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 2021 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'alert("'.str\_replace(G5\_PATH.'/', '',$log\_path).' 폴더에 쓰기권한을 부여해 주십시오.\n> chmod 707 log");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 2042 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'alert("'.str\_replace(G5\_PATH.'/', '',$log\_path).' 폴더에 쓰기권한을 부여해 주십시오.\n> chmod 707 log");'.PHP\_EOL;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$cf\_icode\_server\_port = isset($cf\_icode\_server\_port) ? preg\_replace('/[^0-9]/', '', $cf\_icode\_server\_port) : '7295';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$de\_shop\_skin = isset($\_POST['de\_shop\_skin']) ? preg\_replace('#\.+(\/|\\\)#', '', $\_POST['de\_shop\_skin']) : 'basic';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$de\_shop\_mobile\_skin = isset($\_POST['de\_shop\_mobile\_skin']) ? preg\_replace('#\.+(\/|\\\)#', '', $\_POST['de\_shop\_mobile\_skin']) : 'basic';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$$key = $\_POST[$key] = isset($\_POST[$key]) ? preg\_replace('#\.+(\/|\\\)#', '', strip\_tags($\_POST[$key])) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\configformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$tmps[] = preg\_replace('/[^0-9a-z\_\-]/i', '', $v);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cp\_id" value="<?php echo $cp\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page;?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0"<?php echo get\_selected('0', $cp['cp\_method']); ?>>개별상품할인</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"<?php echo get\_selected('1', $cp['cp\_method']); ?>>카테고리할인</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="2"<?php echo get\_selected('2', $cp['cp\_method']); ?>>주문금액할인</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="3"<?php echo get\_selected('3', $cp['cp\_method']); ?>>배송비할인</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><label for="cp\_target"><?php echo $cp\_target\_label; ?></label></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cp\_target" value="<?php echo stripslashes($cp['cp\_target']); ?>" id="cp\_target" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" id="sch\_target" class="btn\_frmline"><?php echo $cp\_target\_btn; ?></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_id" value="<?php echo stripslashes($cp['mb\_id']); ?>" id="mb\_id" class="frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cp\_start" value="<?php echo stripslashes($cp['cp\_start']); ?>" id="cp\_start" required class="frm\_input required">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cp\_end" value="<?php echo stripslashes($cp['cp\_end']); ?>" id="cp\_end" required class="frm\_input required">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0"<?php echo get\_selected('0', $cp['cp\_type']); ?>>정액할인(원)</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"<?php echo get\_selected('1', $cp['cp\_type']); ?>>정률할인(%)</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><label for="cp\_price"><?php echo $cp['cp\_type'] ? '할인비율' : '할인금액'; ?></label></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cp\_price" value="<?php echo stripslashes($cp['cp\_price']); ?>" id="cp\_price" required class="frm\_input required"> <span id="cp\_price\_unit"><?php echo $cp['cp\_type'] ? '%' : '원'; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"<?php echo get\_selected('1', $cp['cp\_trunc']); ?>>1원단위</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="10"<?php echo get\_selected('10', $cp['cp\_trunc']); ?>>10원단위</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="100"<?php echo get\_selected('100', $cp['cp\_trunc']); ?>>100원단위</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1000"<?php echo get\_selected('1000', $cp['cp\_trunc']); ?>>1,000원단위</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cp\_minimum" value="<?php echo stripslashes($cp['cp\_minimum']); ?>" id="cp\_minimum" class="frm\_input"> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cp\_maximum" value="<?php echo stripslashes($cp['cp\_maximum']); ?>" id="cp\_maximum" class="frm\_input"> 원

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$receive\_number = preg\_replace("/[^0-9]/", "", $arr\_send\_list[$i]['mb\_hp']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace("/[^0-9]/", "", $default['de\_admin\_company\_tel']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">전체 </span><span class="ov\_num"> <?php echo number\_format($total\_count) ?> 개</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mb\_id"<?php echo get\_selected($sfl, "mb\_id"); ?>>회원아이디</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="cp\_subject"<?php echo get\_selected($sfl, "cp\_subject"); ?>>쿠폰이름</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="cp\_id"<?php echo get\_selected($sfl, "cp\_id"); ?>>쿠폰코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx ?>" id="stx" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="cp\_id\_<?php echo $i; ?>" name="cp\_id[<?php echo $i; ?>]" value="<?php echo $row['cp\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="chk\_<?php echo $i; ?>" name="chk[]" value="<?php echo $i; ?>" title="내역선택">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $cp\_method; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $row['cp\_id']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><?php echo $row['cp\_subject']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $cp\_target; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_name sv\_use"><div><?php echo $row['mb\_id']; ?></div></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo substr($row['cp\_start'], 2, 8); ?> ~ <?php echo substr($row['cp\_end'], 2, 8); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_cntsmall"><?php echo number\_format($used\_count); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./couponform.php?w=u&amp;cp\_id=<?php echo $row['cp\_id']; ?>&amp;<?php echo $qstr; ?>" class="btn btn\_03"><span class="sound\_only"><?php echo $row['cp\_id']; ?> </span>수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponlist\_delete.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sql = " delete from {$g5['g5\_shop\_coupon\_table']} where cp\_id = '".preg\_replace('/[^a-z0-9\_\-]/i', '', $\_POST['cp\_id'][$k])."' ";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponmember.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$mb\_name = preg\_replace('/\!\?\\*$#<>()\[\]\{\}/i', '', strip\_tags($mb\_name));

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponmember.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_name" id="mb\_name" value="<?php echo get\_text($mb\_name); ?>" class="frm\_input required" required size="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponmember.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbname"><?php echo get\_text($row['mb\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponmember.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><?php echo $row['mb\_id']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponmember.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="scp\_find\_select td\_mng td\_mng\_s"><button type="button" class="btn btn\_03" onclick="sel\_member\_id('<?php echo $row['mb\_id']; ?>');">선택</button></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponmember.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, '?'.$qstr1.'&amp;page='); ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\coupontarget.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sch\_target = isset($\_GET['sch\_target']) ? substr(preg\_replace('/[^a-zA-Z0-9]/', '', strip\_tags($\_GET['sch\_target'])), 0, 1) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\coupontarget.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1>쿠폰 적용 <?php echo $html\_title; ?>선택</h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\coupontarget.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

쿠폰을 적용할 <?php echo $t\_desc1; ?> 선택하세요.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\coupontarget.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $t\_desc2; ?> 많을 경우에는 검색 기능을 이용하세요.

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\coupontarget.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

<input type="hidden" name="sch\_target" value="<?php echo preg\_replace('/[^a-zA-Z0-9]/', '', strip\_tags($\_GET['sch\_target'])); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\coupontarget.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="sch\_word"><?php echo $t\_name; ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\coupontarget.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="sch\_word" id="sch\_word" value="<?php echo get\_text($sch\_word); ?>" class="frm\_input required" required size="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\coupontarget.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><?php echo $t\_name; ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\coupontarget.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><?php echo $t\_id; ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\coupontarget.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><?php echo $row['t\_name']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\coupontarget.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="scp\_target\_code"><?php echo $row['t\_id']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\coupontarget.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mng td\_mng\_s"><button type="button" class="btn btn\_03" onclick="sel\_target\_id('<?php echo $row['t\_id']; ?>');">선택</button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\coupontarget.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, '?'.$qstr1.'&amp;page='); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cz\_id" value="<?php echo $cz\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page;?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0"<?php echo get\_selected('0', $cp['cz\_type']); ?>>다운로드쿠폰</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"<?php echo get\_selected('1', $cp['cz\_type']); ?>>포인트쿠폰</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cz\_subject" value="<?php echo get\_text($cp['cz\_subject']); ?>" id="cz\_subject" required class="required frm\_input" size="50">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cz\_start" value="<?php echo stripslashes($cp['cz\_start']); ?>" id="cz\_start" required class="frm\_input required">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cz\_end" value="<?php echo stripslashes($cp['cz\_end']); ?>" id="cz\_end" required class="frm\_input required">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cz\_point" value="<?php echo get\_text($cp['cz\_point']); ?>" id="cz\_point" class="frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cz\_period" value="<?php echo stripslashes($cp['cz\_period']); ?>" id="cz\_period" required class="frm\_input required" size="5"> 일

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $cpimg\_str;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0"<?php echo get\_selected('0', $cp['cp\_method']); ?>>개별상품할인</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"<?php echo get\_selected('1', $cp['cp\_method']); ?>>카테고리할인</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="2"<?php echo get\_selected('2', $cp['cp\_method']); ?>>주문금액할인</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="3"<?php echo get\_selected('3', $cp['cp\_method']); ?>>배송비할인</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><label for="cp\_target"><?php echo $cp\_target\_label; ?></label></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cp\_target" value="<?php echo stripslashes($cp['cp\_target']); ?>" id="cp\_target" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" id="sch\_target" class="btn\_frmline"><?php echo $cp\_target\_btn; ?></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0"<?php echo get\_selected('0', $cp['cp\_type']); ?>>정액할인(원)</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"<?php echo get\_selected('1', $cp['cp\_type']); ?>>정률할인(%)</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><label for="cp\_price"><?php echo $cp['cp\_type'] ? '할인비율' : '할인금액'; ?></label></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cp\_price" value="<?php echo stripslashes($cp['cp\_price']); ?>" id="cp\_price" required class="frm\_input required"> <span id="cp\_price\_unit"><?php echo $cp['cp\_type'] ? '%' : '원'; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"<?php echo get\_selected('1', $cp['cp\_trunc']); ?>>1원단위</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 174 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="10"<?php echo get\_selected('10', $cp['cp\_trunc']); ?>>10원단위</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 175 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="100"<?php echo get\_selected('100', $cp['cp\_trunc']); ?>>100원단위</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1000"<?php echo get\_selected('1000', $cp['cp\_trunc']); ?>>1,000원단위</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 183 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cp\_minimum" value="<?php echo stripslashes($cp['cp\_minimum']); ?>" id="cp\_minimum" class="frm\_input"> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 189 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cp\_maximum" value="<?php echo stripslashes($cp['cp\_maximum']); ?>" id="cp\_maximum" class="frm\_input"> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 197 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzoneform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./couponzonelist.php?<?php echo $qstr; ?>" class="btn\_02 btn">목록</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzonelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">전체 </span><span class="ov\_num"> <?php echo number\_format($total\_count) ?> 개</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzonelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx ?>" id="stx" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzonelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzonelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzonelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzonelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzonelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="cz\_id\_<?php echo $i; ?>" name="cz\_id[<?php echo $i; ?>]" value="<?php echo $row['cz\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzonelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="chk\_<?php echo $i; ?>" name="chk[]" value="<?php echo $i; ?>" title="내역선택">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzonelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><?php echo get\_text($row['cz\_subject']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzonelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_type"><?php echo $cz\_type; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzonelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_type"><?php echo $cp\_method; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzonelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_odrnum2"><?php echo $cp\_price; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzonelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_type">다운로드 후 <?php echo $row['cz\_period']; ?>일</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzonelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($row['cz\_download']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzonelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo substr($row['cz\_start'], 2, 8); ?> ~ <?php echo substr($row['cz\_end'], 2, 8); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzonelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./couponzoneform.php?w=u&amp;cz\_id=<?php echo $row['cz\_id']; ?>&amp;<?php echo $qstr; ?>" class="btn btn\_03"><span class="sound\_only"><?php echo get\_text($row['cz\_subject']); ?> </span>수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzonelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\couponzonelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><span></span><?php echo number\_format($val); ?></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php echo $li\_bg; ?>" style="z-index:<?php echo $k; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="graph order" title="<?php echo $order\_title; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 182 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="graph cancel" title="<?php echo $cancel\_title; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 194 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><span></span><?php echo substr($val, 5, 5).' ('.get\_yoil($val).')'; ?></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 209 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 226 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><a href="<?php echo $info['href']; ?>"><?php echo number\_format($info['count']); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 227 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_price"><a href="<?php echo $info['href']; ?>"><?php echo number\_format($info['price']); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 234 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><a href="<?php echo $info['href']; ?>"><?php echo number\_format($info['count']); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 235 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_price"><a href="<?php echo $info['href']; ?>"><?php echo number\_format($info['price']); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 242 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><a href="<?php echo $info['href']; ?>"><?php echo number\_format($info['count']); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 243 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_price"><a href="<?php echo $info['href']; ?>"><?php echo number\_format($info['price']); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 250 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><a href="<?php echo $info['href']; ?>"><?php echo number\_format($info['count']); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 251 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_price"><a href="<?php echo $info['href']; ?>"><?php echo number\_format($info['price']); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 260 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 299 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num2"><a href="./itemstocklist.php"><?php echo number\_format($item\_noti); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 300 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num2"><a href="./optionstocklist.php"><?php echo number\_format($option\_noti); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 301 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_price"><?php echo display\_price(intval($userinfo['coin'])); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 312 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 330 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col" colspan="2"><?php echo $day; ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 352 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" id="th\_val\_<?php echo $val\_cnt; ?>" class="td\_category"><?php echo $val; ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 357 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($info[$date][$val]['count']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 358 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($info[$date][$val]['price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 374 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 393 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="oneq\_cate oneq\_span"><?php echo get\_text($row['qa\_category']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 394 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_BBS\_URL; ?>/qaview.php?qa\_id=<?php echo $row['qa\_id']; ?>" target="\_blank" class="oneq\_link"><?php echo conv\_subject($row['qa\_subject'],40); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 395 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $name; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 413 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 431 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./itemqaform.php?w=u&amp;iq\_id=<?php echo $row['iq\_id']; ?>" class="qna\_link"><?php echo conv\_subject($row['iq\_subject'],40); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 432 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $name; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 450 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 468 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./itemuseform.php?w=u&amp;is\_id=<?php echo $row['is\_id']; ?>" class="ps\_link"><?php echo conv\_subject($row['is\_subject'],40); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 469 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $name; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 473 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<li class="empty\_list">자료가 없습니다.</li>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 521 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var g\_h1 = new Array("<?php echo implode('", "', $h\_val['order']); ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 522 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var g\_h2 = new Array("<?php echo implode('", "', $h\_val['cancel']); ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 191 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

주문일시 <strong><?php echo substr($od['dt\_time'],0,16); ?> (<?php echo get\_yoil($od['dt\_time']); ?>)</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 193 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

주문합계 <strong><?php echo number\_format($order\_price); ?></strong>원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 269 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td rowspan="<?php echo $rowspan; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 270 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $image; ?> <?php echo stripslashes($row['it\_name']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 271 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if(isset($od['od\_tax\_flag']) && $od['od\_tax\_flag'] && $row['ct\_notax']) echo '[비과세상품]'; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 274 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $opt['ct\_option']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 275 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mngsmall"><?php echo $opt['ct\_status']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 276 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($opt['ct\_qty']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 277 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($opt\_price); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 278 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($ct\_price['stotal']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 279 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($opt\_cp\_price); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 280 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($ct\_point['stotal']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 281 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_sendcost\_by"><?php echo $ct\_send\_cost; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 282 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mngsmall"><?php echo get\_yn($opt['ct\_point\_use']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 283 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mngsmall"><?php echo get\_yn($opt['ct\_stock\_use']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 298 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 342 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_id" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 343 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 344 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 345 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 346 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 347 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 349 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="sodr\_nonpay">미수금 <?php echo display\_price($amount['misu']); ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 367 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od['od\_id']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 368 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_paybybig"><?php echo $s\_receipt\_way; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 369 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig td\_numsum"><?php echo display\_price($amount['order']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 370 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig"><?php echo display\_price($od\_send\_cost + $od\_send\_cost2); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 371 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig"><?php echo display\_point($od\_temp\_point); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 372 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig td\_numincome"><?php echo number\_format($amount['receipt']); ?>원</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 373 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig td\_numcoupon"><?php echo display\_price($amount['coupon']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 374 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig td\_numcancel"><?php echo number\_format($amount['cancel']); ?>원</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 426 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $tmp['oid']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 430 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $tmp['P\_TID']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 434 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $tmp['P\_MID']; ?><?php echo in\_array( strtolower($tmp['P\_MID']), array('iniescrow0', 'inipaytest') ) ? ' ( 테스트결제 )' : ''; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 438 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo date('Y-m-d H:i:s', strtotime(substr($tmp['P\_AUTH\_DT'], 0, 14))); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 442 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $tmp['P\_TYPE'].' '.$tmp['P\_FN\_NM']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 446 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $tmp['P\_AMT'] ? number\_format($tmp['P\_AMT']) : 0; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 458 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 475 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($data['od\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 479 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($data['od\_tel']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 483 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($data['od\_hp']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 488 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $data['od\_zip']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 489 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo get\_text($data['od\_addr1']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 490 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo get\_text($data['od\_addr2']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 491 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo get\_text($data['od\_addr3']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 496 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($data['od\_email']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 516 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($data['od\_b\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 520 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($data['od\_b\_tel']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 524 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($data['od\_b\_hp']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 529 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $data['od\_b\_zip']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 530 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo get\_text($data['od\_b\_addr1']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 531 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo get\_text($data['od\_b\_addr2']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 532 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo get\_text($data['od\_b\_addr3']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 539 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $data['od\_hope\_date']; ?> (<?php echo get\_yoil($data['od\_hope\_date']); ?>)</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 544 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php if ($data['od\_memo']) echo get\_text($data['od\_memo'], 1);else echo "없음";?></td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 218 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_zip = preg\_replace('/[^0-9]/', '', $data['od\_zip']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 228 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_b\_zip = preg\_replace('/[^0-9]/', '', $data['od\_b\_zip']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 390 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderformupdate.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'document.location.href = "./orderform.php?od\_id='.$od\_id.'";'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 392 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderformupdate.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'document.location.href = "./inorderlist.php?'.str\_replace('&amp;', '&', $qstr).'";'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">전체 </span><span class="ov\_num"> <?php echo number\_format($total\_count) ?> 건 </span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="od\_id"<?php echo get\_selected($sfl, "od\_id"); ?>>주문번호</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx ?>" id="stx" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="od\_id\_<?php echo $i; ?>" name="od\_id[<?php echo $i; ?>]" value="<?php echo $row['od\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="chk\_<?php echo $i; ?>" name="chk[]" value="<?php echo $i; ?>" title="내역선택">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_odrnum2"><?php echo $row['od\_id']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_center"><?php echo $pg; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_name"><?php echo get\_text($data['od\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_center"><?php echo get\_text($data['od\_tel']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_name"><?php echo get\_text($data['od\_b\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_price"><?php echo number\_format($ct['price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_center"><?php echo $data['od\_settle\_case']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_time"><?php echo $row['dt\_time']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./inorderform.php?od\_id=<?php echo $row['od\_id']; ?>&amp;<?php echo $qstr; ?>" class="btn btn\_03"><span class="sound\_only"><?php echo $row['od\_id']; ?> </span>보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./inorderformupdate.php?w=d&amp;od\_id=<?php echo $row['od\_id']; ?>&amp;<?php echo $qstr; ?>" onclick="return delete\_confirm(this);" class="btn btn\_02"><span class="sound\_only"><?php echo $row['od\_id']; ?> </span>삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\inorderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 5 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemcopy.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ca\_id = isset($\_REQUEST['ca\_id']) ? preg\_replace('/[^0-9a-z]/i', '', $\_REQUEST['ca\_id']) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemcopy.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="button" value="복사하기" class="btn\_submit" onclick="\_copy('itemcopyupdate.php?it\_id=<?php echo $it\_id; ?>&amp;ca\_id=<?php echo $ca\_id; ?>');">

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemcopyupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ca\_id = isset($\_REQUEST['ca\_id']) ? preg\_replace('/[^0-9a-z]/i', '', $\_REQUEST['ca\_id']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemcopyupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$new\_it\_id = isset($\_REQUEST['new\_it\_id']) ? preg\_replace("/[^A-Za-z0-9\-\_]/", "", $\_REQUEST['new\_it\_id']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemcopyupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$src\_path = preg\_replace("/^\/.\*\/data/", "/data", $p['path']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemcopyupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$dstfile = preg\_replace("/\.([^\.]+)$/", "\_".$new\_it\_id.".\\1", $srcfile);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemcopyupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$newfile = preg\_replace("/\.([^\.]+)$/", "\_".$new\_it\_id.".\\1", $matchs[1][$i]);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemcopyupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$src\_path = preg\_replace("/^\/.\*\/data/", "/data", $p['path']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemcopyupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$dstfile = preg\_replace("/\.([^\.]+)$/", "\_".$new\_it\_id.".\\1", $srcfile);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemcopyupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$newfile = preg\_replace("/\.([^\.]+)$/", "\_".$new\_it\_id.".\\1", $matchs[1][$i]);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemdelete.inc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$data\_path = preg\_replace("/^\/.\*\/data/", "/data", $p['path']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemdelete.inc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$data\_path = preg\_replace("/^\/.\*\/data/", "/data", $p['path']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemevent.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">전체 이벤트</span><span class="ov\_num"> <?php echo $total\_count; ?>건</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemevent.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemevent.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['ev\_id']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemevent.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><?php echo $subject; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemevent.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $href; ?><?php echo $ev['cnt']; ?><?php echo $href\_close; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemevent.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_boolean"><?php echo $row['ev\_use'] ? '<span class="txt\_true">예</span>' : '<span class="txt\_false">아니오</span>'; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemevent.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./itemeventform.php?w=u&amp;ev\_id=<?php echo $row['ev\_id']; ?>" class="btn btn\_03">수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemevent.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_SHOP\_URL; ?>/event.php?ev\_id=<?php echo $row['ev\_id']; ?>" class="btn btn\_02">보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemevent.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./itemeventformupdate.php?w=d&amp;ev\_id=<?php echo $row['ev\_id']; ?>" onclick="return delete\_confirm(this);" class="btn btn\_02">삭제</a>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ev\_id = isset($\_REQUEST['ev\_id']) ? preg\_replace('/[^0-9]/', '', $\_REQUEST['ev\_id']) : '';

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_event\_table']}`

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ev\_id" value="<?php echo $ev\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="frm\_ev\_id"><?php echo $ev\_id; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_SHOP\_URL; ?>/event.php?ev\_id=<?php echo $ev['ev\_id']; ?>" class="btn\_frmline">이벤트바로가기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^list.[0-9]+\.skin\.php", G5\_SHOP\_SKIN\_PATH, $ev['ev\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_list\_skin\_options("^list.[0-9]+\.skin\.php", G5\_MSHOP\_SKIN\_PATH, $ev['ev\_mobile\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ev\_img\_width" value="<?php echo $ev['ev\_img\_width']; ?>" id="ev\_img\_width" required class="required frm\_input" size="5"> 픽셀

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ev\_img\_height" value="<?php echo $ev['ev\_img\_height']; ?>" id="ev\_img\_height" required class="required frm\_input" size="5"> 픽셀

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ev\_list\_mod" value="<?php echo $ev['ev\_list\_mod']; ?>" id="ev\_list\_mod" required class="required frm\_input" size="3"> 개

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ev\_list\_row" value="<?php echo $ev['ev\_list\_row']; ?>" id="ev\_list\_row" required class="required frm\_input" size="3"> 줄

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ev\_mobile\_img\_width" value="<?php echo $ev['ev\_mobile\_img\_width']; ?>" id="ev\_mobile\_img\_width" required class="required frm\_input" size="5"> 픽셀

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ev\_mobile\_img\_height" value="<?php echo $ev['ev\_mobile\_img\_height']; ?>" id="ev\_mobile\_img\_height" required class="required frm\_input" size="5"> 픽셀

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ev\_mobile\_list\_mod" value="<?php echo $ev['ev\_mobile\_list\_mod']; ?>" id="ev\_mobile\_list\_mod" required class="required frm\_input" size="3"> 개

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 172 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ev\_mobile\_list\_row" value="<?php echo $ev['ev\_mobile\_list\_row']; ?>" id="ev\_mobile\_list\_row" required class="required frm\_input" size="3"> 개

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($ev['ev\_use'], 1); ?>>사용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 181 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected($ev['ev\_use'], 0); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ev\_subject" value="<?php echo htmlspecialchars2($ev['ev\_subject']); ?>" id="ev\_subject" required class="required frm\_input" size="60">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 189 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="ev\_subject\_strong" value="1" id="ev\_subject\_strong" <?php if($ev['ev\_subject\_strong']) echo 'checked="checked"'; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 213 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $mimg\_str;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 228 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_select; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 252 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[]" value="<?php echo $row['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 253 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="list\_item"><?php echo $it\_name; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 288 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $himg\_str;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 313 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $timg\_str;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 322 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo editor\_html('ev\_head\_html', get\_text(html\_purifier($ev['ev\_head\_html']), 0)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 328 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo editor\_html('ev\_tail\_html', get\_text(html\_purifier($ev['ev\_tail\_html']), 0)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 381 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

{ w: "<?php echo $w; ?>", ev\_id: "<?php echo $ev\_id; ?>", ca\_id: ca\_id, it\_name: it\_name }

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ev\_skin = preg\_replace('#\.+(\/|\\\)#', '', $ev\_skin);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ev\_mobile\_skin = preg\_replace('#\.+(\/|\\\)#', '', $ev\_mobile\_skin);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ev\_id = isset($\_GET['ev\_id']) ? preg\_replace('/[^0-9]/', '', $\_GET['ev\_id']) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">전체 이벤트</span><span class="ov\_num"> <?php echo $total\_count; ?>건</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="ev\_id" id="ev\_id" action="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $event\_option;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ev\_id" value="<?php echo $ev\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<option value="'.$row1['ca\_id'].'" '.get\_selected($sel\_ca\_id, $row1['ca\_id']).'>'.$nbsp.$row1['ca\_name'].'</option>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="it\_name" <?php echo get\_selected($sel\_field, 'it\_name'); ?>>상품명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.it\_id" <?php echo get\_selected($sel\_field, 'a.it\_id'); ?>>상품코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="search" value="<?php echo $search; ?>" id="search" required class="frm\_input required">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p>상품을 이벤트별로 일괄 처리합니다. <?php echo ($ev\_title ? '현재 선택된 이벤트는 '.$ev\_title.'입니다.' : '이벤트를 선택해 주세요.'); ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ev\_id" value="<?php echo $ev\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sel\_ca\_id" value="<?php echo $sel\_ca\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sel\_field" value="<?php echo $sel\_field; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="search" value="<?php echo $search; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort1" value="<?php echo $sort1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort2" value="<?php echo $sort2; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("a.it\_id") . '&amp;'.$qstr1.'&amp;ev\_id='.$ev\_id; ?>">상품코드</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("it\_name") . '&&amp;'.$qstr1.'&amp;ev\_id='.$ev\_id; ?>">상품명</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[<?php echo $i; ?>]" value="<?php echo $row['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ev\_chk\_<?php echo $i; ?>" class="sound\_only">이벤트 사용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="ev\_chk[<?php echo $i; ?>]" value="1" id="ev\_chk\_<?php echo $i; ?>" <?php echo ($row['ev\_id'] ? "checked" : ""); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><a href="<?php echo $href; ?>"><?php echo $row['it\_id']; ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 169 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><a href="<?php echo $href; ?>"><?php echo get\_it\_image($row['it\_id'], 50, 50); ?> <?php echo cut\_str(stripslashes($row['it\_name']), 60, "&#133"); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 185 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

현재 선택된 이벤트는 <strong><?php echo $ev\_title; ?></strong>입니다.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 199 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventlistupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$iit\_id = isset($\_POST['it\_id'][$i]) ? preg\_replace('/[^a-z0-9\_\-]/i', '', $\_POST['it\_id'][$i]) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventsearch.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventwin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title']; ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventwin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 입력</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventwin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $href; ?>" target="\_blank">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventwin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_it\_image($row['it\_id'], 40, 40); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventwin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo cut\_str(stripslashes($row['it\_name']), 60, "&#133"); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventwin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_boolean"><?php echo ($row['it\_use']?"사용":"미사용"); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemeventwin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mngsmall"><a href="javascript:del('./itemeventwindel.php?ev\_id=<?php echo $ev\_id; ?>&amp;it\_id=<?php echo $row['it\_id']; ?>');">삭제</a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemexcel.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title']; ?></h1>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemexcelupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace('/[^0-9]/', '', $n);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemexcelupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$it\_id = preg\_match('/[-+]?[0-9]\*\.?[0-9]+([eE][-+]?[0-9]+)/', $it\_id) ? addslashes(sprintf("%.0f", $it\_id)) : preg\_replace('/[^0-9a-z\_\-]/i', '', $it\_id);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemexcelupdate.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title']; ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 181 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemexcelupdate.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo number\_format($total\_count); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 183 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemexcelupdate.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo number\_format($succ\_count); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 185 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemexcelupdate.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo number\_format($fail\_count); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemexcelupdate.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo implode(', ', $fail\_it\_id); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 192 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemexcelupdate.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo number\_format($dup\_count); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 194 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemexcelupdate.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo implode(', ', $dup\_it\_id); ?></dd>

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_item\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_item\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_item\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_item\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 199 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_item\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 205 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_item\_table']}`

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 213 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 214 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 215 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 216 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 217 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 218 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 219 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 223 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 239 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($w == "") echo help("기본분류를 선택하면, 판매/재고/HTML사용/판매자 E-mail 등을, 선택한 분류의 기본값으로 설정합니다."); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 242 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_selected\_option($category\_select, $it['ca\_id']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 255 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo "\n$script"; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 261 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><label for="ca\_id<?php echo $i; ?>"><?php echo $i; ?>차 분류</label></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 263 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo help($i.'차 분류는 기본 분류의 하위 분류 개념이 아니므로 기본 분류 선택시 해당 상품이 포함될 최하위 분류만 선택하시면 됩니다.'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 264 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="ca\_id<?php echo $i; ?>" id="ca\_id<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 266 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_selected\_option($category\_select, $it['ca\_id'.$i]); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 279 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 292 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_skin\_select('shop', 'it\_skin', 'it\_skin', $it['it\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 304 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_mobile\_skin\_select('shop', 'it\_mobile\_skin', 'it\_mobile\_skin', $it['it\_mobile\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 321 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 338 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id" value="<?php echo $it['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 339 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="frm\_ca\_id"><?php echo $it['it\_id']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 340 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo shop\_item\_url($it\_id); ?>" class="btn\_frmline">상품확인</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 341 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_ADMIN\_URL; ?>/shop\_admin/itemuselist.php?sfl=a.it\_id&amp;stx=<?php echo $it\_id; ?>" class="btn\_frmline">사용후기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 342 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_ADMIN\_URL; ?>/shop\_admin/itemqalist.php?sfl=a.it\_id&amp;stx=<?php echo $it\_id; ?>" class="btn\_frmline">상품문의</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 350 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_name" value="<?php echo get\_text(cut\_str($it['it\_name'], 250, "")); ?>" id="it\_name" required class="frm\_input required" size="95">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 357 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_basic" value="<?php echo get\_text(html\_purifier($it['it\_basic'])); ?>" id="it\_basic" class="frm\_input" size="95">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 370 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_order" value="<?php echo $it['it\_order']; ?>" id="it\_order" class="frm\_input" size="12">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 383 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_type1" value="1" <?php echo ($it['it\_type1'] ? "checked" : ""); ?> id="it\_type1">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 385 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_type2" value="1" <?php echo ($it['it\_type2'] ? "checked" : ""); ?> id="it\_type2">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 387 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_type3" value="1" <?php echo ($it['it\_type3'] ? "checked" : ""); ?> id="it\_type3">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 389 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_type4" value="1" <?php echo ($it['it\_type4'] ? "checked" : ""); ?> id="it\_type4">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 391 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_type5" value="1" <?php echo ($it['it\_type5'] ? "checked" : ""); ?> id="it\_type5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 405 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_maker" value="<?php echo get\_text($it['it\_maker']); ?>" id="it\_maker" class="frm\_input" size="40">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 418 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_origin" value="<?php echo get\_text($it['it\_origin']); ?>" id="it\_origin" class="frm\_input" size="40">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 431 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_brand" value="<?php echo get\_text($it['it\_brand']); ?>" id="it\_brand" class="frm\_input" size="40">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 444 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_model" value="<?php echo get\_text($it['it\_model']); ?>" id="it\_model" class="frm\_input" size="40">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 457 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_tel\_inq" value="1" id="it\_tel\_inq" <?php echo ($it['it\_tel\_inq']) ? "checked" : ""; ?>> 예

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 470 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_use" value="1" id="it\_use" <?php echo ($it['it\_use']) ? "checked" : ""; ?>> 예

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 483 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_nocoupon" value="1" id="it\_nocoupon" <?php echo ($it['it\_nocoupon']) ? "checked" : ""; ?>> 예

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 496 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ec\_mall\_pid" value="<?php echo get\_text($it['ec\_mall\_pid']); ?>" id="ec\_mall\_pid" class="frm\_input" size="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 501 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="2"> <?php echo editor\_html('it\_explan', get\_text(html\_purifier($it['it\_explan']), 0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 505 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="2"> <?php echo editor\_html('it\_mobile\_explan', get\_text(html\_purifier($it['it\_mobile\_explan']), 0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 522 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><textarea name="it\_shop\_memo" id="it\_shop\_memo"><?php echo html\_purifier($it['it\_shop\_memo']); ?></textarea></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 538 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 552 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<option value="'.$opt\_value.'" '.get\_selected($opt\_value, $it['it\_info\_gubun']).'>'.$opt\_text.'</option>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 567 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

{ it\_id: "<?php echo $it['it\_id']; ?>", gubun: gubun },

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 578 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 592 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_price" value="<?php echo $it['it\_price']; ?>" id="it\_price" class="frm\_input" size="8"> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 605 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_cust\_price" value="<?php echo $it['it\_cust\_price']; ?>" id="it\_cust\_price" class="frm\_input" size="8"> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 619 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0"<?php echo get\_selected('0', $it['it\_point\_type']); ?>>설정금액</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 620 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"<?php echo get\_selected('1', $it['it\_point\_type']); ?>>판매가기준 설정비율</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 621 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="2"<?php echo get\_selected('2', $it['it\_point\_type']); ?>>구매가기준 설정비율</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 645 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_point" value="<?php echo $it['it\_point']; ?>" id="it\_point" class="frm\_input" size="8"> <span id="it\_point\_unit"><?php if($it['it\_point\_type']) echo '%'; else echo '점'; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 658 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_supply\_point" value="<?php echo $it['it\_supply\_point']; ?>" id="it\_supply\_point" class="frm\_input" size="8"> 점

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 671 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_soldout" value="1" id="it\_soldout" <?php echo ($it['it\_soldout']) ? "checked" : ""; ?>> 예

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 684 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_stock\_sms" value="1" id="it\_stock\_sms" <?php echo ($it['it\_stock\_sms']) ? "checked" : ""; ?>> 예

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 691 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_stock\_qty" value="<?php echo $it['it\_stock\_qty']; ?>" id="it\_stock\_qty" class="frm\_input" size="8"> 개

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 704 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_noti\_qty" value="<?php echo $it['it\_noti\_qty']; ?>" id="it\_noti\_qty" class="frm\_input" size="8"> 개

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 717 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_buy\_min\_qty" value="<?php echo $it['it\_buy\_min\_qty']; ?>" id="it\_buy\_min\_qty" class="frm\_input" size="8"> 개

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 730 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_buy\_max\_qty" value="<?php echo $it['it\_buy\_max\_qty']; ?>" id="it\_buy\_max\_qty" class="frm\_input" size="8"> 개

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 744 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0"<?php echo get\_selected('0', $it['it\_notax']); ?>>과세</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 745 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"<?php echo get\_selected('1', $it['it\_notax']); ?>>비과세</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 773 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="opt1\_subject" value="<?php echo isset($opt\_subject[0]) ? $opt\_subject[0] : ''; ?>" id="opt1\_subject" class="frm\_input" size="15">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 783 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="opt2\_subject" value="<?php echo isset($opt\_subject[1]) ? $opt\_subject[1] : ''; ?>" id="opt2\_subject" class="frm\_input" size="15">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 793 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="opt3\_subject" value="<?php echo isset($opt\_subject[2]) ? $opt\_subject[2] : ''; ?>" id="opt3\_subject" class="frm\_input" size="15">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 857 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

{ it\_id: it\_id, w: "<?php echo $w; ?>", opt1\_subject: opt1\_subject, opt2\_subject: opt2\_subject, opt3\_subject: opt3\_subject, opt1: opt1, opt2: opt2, opt3: opt3 },

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 956 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="spl\_subject\_<?php echo $seq; ?>">추가<?php echo $seq; ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 957 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="spl\_subject[]" id="spl\_subject\_<?php echo $seq; ?>" value="<?php echo $spl\_subject[$i]; ?>" class="frm\_input" size="15">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 960 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="spl\_item\_<?php echo $seq; ?>"><b>추가<?php echo $seq; ?> 항목</b></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 961 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="spl[]" id="spl\_item\_<?php echo $seq; ?>" value="" class="frm\_input" size="40">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1063 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

{ it\_id: it\_id, w: "<?php echo $w; ?>", 'subject[]': subject, 'supply[]': supply },

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1182 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0"<?php echo get\_selected('0', $it['it\_sc\_type']); ?>>쇼핑몰 기본설정 사용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1183 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"<?php echo get\_selected('1', $it['it\_sc\_type']); ?>>무료배송</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1184 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="2"<?php echo get\_selected('2', $it['it\_sc\_type']); ?>>조건부 무료배송</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1185 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="3"<?php echo get\_selected('3', $it['it\_sc\_type']); ?>>유료배송</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1186 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="4"<?php echo get\_selected('4', $it['it\_sc\_type']); ?>>수량별 부과</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1200 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0"<?php echo get\_selected('0', $it['it\_sc\_method']); ?>>선불</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1201 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"<?php echo get\_selected('1', $it['it\_sc\_method']); ?>>착불</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1202 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="2"<?php echo get\_selected('2', $it['it\_sc\_method']); ?>>사용자선택</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1210 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_sc\_price" value="<?php echo $it['it\_sc\_price']; ?>" id="it\_sc\_price" class="frm\_input" size="8"> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1216 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

주문금액 <input type="text" name="it\_sc\_minimum" value="<?php echo $it['it\_sc\_minimum']; ?>" id="it\_sc\_minimum" class="frm\_input" size="8"> 이상 무료 배송

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1223 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

주문수량 <input type="text" name="it\_sc\_qty" value="<?php echo $it['it\_sc\_qty']; ?>" id="it\_sc\_qty" class="frm\_input" size="8"> 마다 배송비 부과

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1235 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_method").hide();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_basic").hide();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1237 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_minimum").hide();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1238 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_qty").hide();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1239 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_grp").attr("rowspan","1");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1242 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_method").show();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1243 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_basic").show();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1244 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_minimum").show();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1245 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_qty").hide();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1246 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_grp").attr("rowspan","4");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1249 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_method").show();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1250 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_basic").show();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1251 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_minimum").hide();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1252 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_qty").hide();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1253 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_grp").attr("rowspan","3");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1256 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_method").show();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1257 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_basic").show();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1258 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_minimum").hide();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1259 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_qty").show();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1260 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_grp").attr("rowspan","4");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1263 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_method").hide();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1264 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_basic").hide();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1265 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_minimum").hide();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1266 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_con\_qty").hide();'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1267 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '$("#sc\_grp").attr("rowspan","2");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1319 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1331 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><label for="it\_img<?php echo $i; ?>">이미지 <?php echo $i; ?></label></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1333 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="file" name="it\_img<?php echo $i; ?>" id="it\_img<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1342 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="it\_img<?php echo $i; ?>\_del"><span class="sound\_only">이미지 <?php echo $i; ?> </span>파일삭제</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1343 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_img<?php echo $i; ?>\_del" id="it\_img<?php echo $i; ?>\_del" value="1">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1344 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sit\_wimg\_limg<?php echo $i; ?>"><?php echo $thumb; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1345 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="limg<?php echo $i; ?>" class="banner\_or\_img">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1346 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $img\_tag; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1350 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$('<button type="button" id="it\_limg<?php echo $i; ?>\_view" class="btn\_frmline sit\_wimg\_view">이미지<?php echo $i; ?> 확인</button>').appendTo('.sit\_wimg\_limg<?php echo $i; ?>');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1364 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1395 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<option value=\"{$row['ca\_id']}\">$nbsp{$row['ca\_name']}</option>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1420 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

{ it\_id: "<?php echo $it\_id; ?>", ca\_id: ca\_id, it\_name: it\_name }

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1489 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="re\_it\_id[]" value="<?php echo $row['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1490 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="list\_item"><?php echo $it\_name; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1504 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_list" value="<?php echo $str; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1514 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1528 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ev\_id[]" value="<?php echo $row['ev\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1529 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="list\_item"><?php echo get\_text($row['ev\_subject']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1606 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ev\_id[]" value="<?php echo $row['ev\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1607 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="list\_item"><?php echo get\_text($row['ev\_subject']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1619 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ev\_list" value="<?php echo $str; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1628 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1641 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo help("상품상세설명 페이지 상단에 출력하는 HTML 내용입니다."); ?><?php echo editor\_html('it\_head\_html', get\_text(html\_purifier($it['it\_head\_html']), 0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1651 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo help("상품상세설명 페이지 하단에 출력하는 HTML 내용입니다."); ?><?php echo editor\_html('it\_tail\_html', get\_text(html\_purifier($it['it\_tail\_html']), 0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1661 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo help("모바일 상품상세설명 페이지 상단에 출력하는 HTML 내용입니다."); ?><?php echo editor\_html('it\_mobile\_head\_html', get\_text(html\_purifier($it['it\_mobile\_head\_html']), 0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1671 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo help("모바일 상품상세설명 페이지 하단에 출력하는 HTML 내용입니다."); ?><?php echo editor\_html('it\_mobile\_tail\_html', get\_text(html\_purifier($it['it\_mobile\_tail\_html']), 0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1687 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1699 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row">여분필드<?php echo $i ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1701 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="it\_<?php echo $i ?>\_subj">여분필드 <?php echo $i ?> 제목</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1702 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_<?php echo $i ?>\_subj" id="it\_<?php echo $i ?>\_subj" value="<?php echo get\_text($it['it\_'.$i.'\_subj']) ?>" class="frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1703 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="it\_<?php echo $i ?>">여분필드 <?php echo $i ?> 값</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1704 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_<?php echo $i ?>" value="<?php echo get\_text($it['it\_'.$i]) ?>" id="it\_<?php echo $i ?>" class="frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1707 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_ca\_<?php echo $i ?>" value="1" id="chk\_ca\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1708 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_ca\_<?php echo $i ?>">분류적용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1709 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_all\_<?php echo $i ?>" value="1" id="chk\_all\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1710 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_all\_<?php echo $i ?>">전체적용</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1719 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $it['it\_time']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1726 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $it['it\_update\_time']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1736 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./itemlist.php?<?php echo $qstr; ?>" class="btn btn\_02">목록</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1737 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo shop\_item\_url($it\_id); ?>" class="btn\_02 btn">상품보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemformrelation.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ca\_id = isset($\_POST['ca\_id']) ? preg\_replace('/[^0-9a-z]/i', '', $\_POST['ca\_id']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ca\_id2 = isset($\_POST['ca\_id2']) ? preg\_replace('/[^0-9a-z]/i', '', $\_POST['ca\_id2']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ca\_id3 = isset($\_POST['ca\_id3']) ? preg\_replace('/[^0-9a-z]/i', '', $\_POST['ca\_id3']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 246 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$post\_opt\_id = isset($\_POST['opt\_id'][$i]) ? preg\_replace(G5\_OPTION\_ID\_FILTER, '', strip\_tags($\_POST['opt\_id'][$i])) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 274 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$post\_spl\_id = isset($\_POST['spl\_id'][$i]) ? preg\_replace(G5\_OPTION\_ID\_FILTER, '', strip\_tags($\_POST['spl\_id'][$i])) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 334 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$it\_basic = preg\_replace('#<script(.\*?)>(.\*?)<\/script>#is', '', $it\_basic);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 432 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$t\_it\_id = preg\_replace("/[A-Za-z0-9\-\_]/", "", $it\_id);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 652 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemformupdate.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

location.href = "<?php echo "./itemform.php?".str\_replace('&amp;', '&', $qstr); ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 654 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemformupdate.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

location.href = "<?php echo "./itemlist.php?".str\_replace('&amp;', '&', $qstr); ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\iteminfo.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><label for="ii\_article\_<?php echo $el\_name; ?>"><?php echo $el\_title; ?></label></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\iteminfo.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ii\_article[]" value="<?php echo $el\_name; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\iteminfo.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($el\_example != "") echo help($el\_example); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\iteminfo.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ii\_value[]" value="<?php echo get\_text($el\_value); ?>" id="ii\_article\_<?php echo $el\_name; ?>" required class="frm\_input required" />

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\iteminfo.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td rowspan="<?php echo $el\_length; ?>" class="td\_grpset">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">등록된 상품</span><span class="ov\_num"> <?php echo $total\_count; ?>건</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="save\_stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<option value="'.$row1['ca\_id'].'" '.get\_selected($sca, $row1['ca\_id']).'>'.$nbsp.$row1['ca\_name'].'</option>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="it\_name" <?php echo get\_selected($sfl, 'it\_name'); ?>>상품명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="it\_id" <?php echo get\_selected($sfl, 'it\_id'); ?>>상품코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="it\_maker" <?php echo get\_selected($sfl, 'it\_maker'); ?>>제조사</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="it\_origin" <?php echo get\_selected($sfl, 'it\_origin'); ?>>원산지</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="it\_sell\_email" <?php echo get\_selected($sfl, 'it\_sell\_email'); ?>>판매자 e-mail</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx; ?>" id="stx" class="frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col" rowspan="3"><?php echo subject\_sort\_link('it\_id', 'sca='.$sca); ?>상품코드</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col" rowspan="3"><?php echo subject\_sort\_link('it\_order', 'sca='.$sca); ?>순서</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col" rowspan="3"><?php echo subject\_sort\_link('it\_use', 'sca='.$sca, 1); ?>판매</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col" rowspan="3"><?php echo subject\_sort\_link('it\_soldout', 'sca='.$sca, 1); ?>품절</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col" rowspan="3"><?php echo subject\_sort\_link('it\_hit', 'sca='.$sca, 1); ?>조회</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col" rowspan="2" id="th\_pc\_title"><?php echo subject\_sort\_link('it\_name', 'sca='.$sca); ?>상품명</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col" id="th\_amt"><?php echo subject\_sort\_link('it\_price', 'sca='.$sca); ?>판매가격</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col" id="th\_camt"><?php echo subject\_sort\_link('it\_cust\_price', 'sca='.$sca); ?>시중가격</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col" id="th\_pt"><?php echo subject\_sort\_link('it\_point', 'sca='.$sca); ?>포인트</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col" id="th\_qty"><?php echo subject\_sort\_link('it\_stock\_qty', 'sca='.$sca); ?>재고</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i; ?>" class="sound\_only"><?php echo get\_text($row['it\_name']); ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk[]" value="<?php echo $i ?>" id="chk\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 174 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[<?php echo $i; ?>]" value="<?php echo $row['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 175 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $row['it\_id']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_id\_<?php echo $i; ?>" class="sound\_only"><?php echo get\_text($row['it\_name']); ?> 기본분류</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="ca\_id[<?php echo $i; ?>]" id="ca\_id\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_selected\_option($ca\_list, $row['ca\_id']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 182 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_id2\_<?php echo $i; ?>" class="sound\_only"><?php echo get\_text($row['it\_name']); ?> 2차분류</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 183 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="ca\_id2[<?php echo $i; ?>]" id="ca\_id2\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 184 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_selected\_option($ca\_list, $row['ca\_id2']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 186 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ca\_id3\_<?php echo $i; ?>" class="sound\_only"><?php echo get\_text($row['it\_name']); ?> 3차분류</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="ca\_id3[<?php echo $i; ?>]" id="ca\_id3\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_selected\_option($ca\_list, $row['ca\_id3']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 192 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="order\_<?php echo $i; ?>" class="sound\_only">순서</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 193 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_order[<?php echo $i; ?>]" value="<?php echo $row['it\_order']; ?>" id="order\_<?php echo $i; ?>" class="tbl\_input" size="3">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 196 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="use\_<?php echo $i; ?>" class="sound\_only">판매여부</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 197 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_use[<?php echo $i; ?>]" <?php echo ($row['it\_use'] ? 'checked' : ''); ?> value="1" id="use\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 200 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="soldout\_<?php echo $i; ?>" class="sound\_only">품절</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 201 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_soldout[<?php echo $i; ?>]" <?php echo ($row['it\_soldout'] ? 'checked' : ''); ?> value="1" id="soldout\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 203 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td rowspan="3" class="td\_num"><?php echo $row['it\_hit']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 205 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./itemform.php?w=u&amp;it\_id=<?php echo $row['it\_id']; ?>&amp;ca\_id=<?php echo $row['ca\_id']; ?>&amp;<?php echo $qstr; ?>" class="btn btn\_03"><span class="sound\_only"><?php echo htmlspecialchars2(cut\_str($row['it\_name'],250, "")); ?> </span>수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 206 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./itemcopy.php?it\_id=<?php echo $row['it\_id']; ?>&amp;ca\_id=<?php echo $row['ca\_id']; ?>" class="itemcopy btn btn\_02" target="\_blank"><span class="sound\_only"><?php echo htmlspecialchars2(cut\_str($row['it\_name'],250, "")); ?> </span>복사</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 207 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $href; ?>" class="btn btn\_02"><span class="sound\_only"><?php echo htmlspecialchars2(cut\_str($row['it\_name'],250, "")); ?> </span>보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 210 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 211 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td rowspan="2" class="td\_img"><a href="<?php echo $href; ?>"><?php echo get\_it\_image($row['it\_id'], 50, 50); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 213 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="name\_<?php echo $i; ?>" class="sound\_only">상품명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 214 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_name[<?php echo $i; ?>]" value="<?php echo htmlspecialchars2(cut\_str($row['it\_name'],250, "")); ?>" id="name\_<?php echo $i; ?>" required class="tbl\_input required" size="30">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 217 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="price\_<?php echo $i; ?>" class="sound\_only">판매가격</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 218 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_price[<?php echo $i; ?>]" value="<?php echo $row['it\_price']; ?>" id="price\_<?php echo $i; ?>" class="tbl\_input sit\_amt" size="7">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 221 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="cust\_price\_<?php echo $i; ?>" class="sound\_only">시중가격</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 222 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_cust\_price[<?php echo $i; ?>]" value="<?php echo $row['it\_cust\_price']; ?>" id="cust\_price\_<?php echo $i; ?>" class="tbl\_input sit\_camt" size="7">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 225 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="it\_skin\_<?php echo $i; ?>" class="sound\_only">PC 스킨</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 226 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_skin\_select('shop', 'it\_skin\_'.$i, 'it\_skin['.$i.']', $row['it\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 229 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 230 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_pt" class="td\_numbig td\_input"><?php echo $it\_point; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 232 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="stock\_qty\_<?php echo $i; ?>" class="sound\_only">재고</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 233 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_stock\_qty[<?php echo $i; ?>]" value="<?php echo $row['it\_stock\_qty']; ?>" id="stock\_qty\_<?php echo $i; ?>" class="tbl\_input sit\_qty" size="7">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="it\_mobile\_skin\_<?php echo $i; ?>" class="sound\_only">모바일 스킨</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 237 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_mobile\_skin\_select('shop', 'it\_mobile\_skin\_'.$i, 'it\_mobile\_skin['.$i.']', $row['it\_mobile\_skin']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 263 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlistupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$p\_it\_id = isset($\_POST['it\_id'][$k]) ? preg\_replace('/[^a-z0-9\_\-]/i', '', $\_POST['it\_id'][$k]) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemlistupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$it\_id = isset($\_POST['it\_id'][$k]) ? preg\_replace('/[^a-z0-9\_\-]/i', '', $\_POST['it\_id'][$k]) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$opt1\_subject = isset($\_POST['opt1\_subject']) ? preg\_replace(G5\_OPTION\_ID\_FILTER, '', trim(stripslashes($\_POST['opt1\_subject']))) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$opt2\_subject = isset($\_POST['opt2\_subject']) ? preg\_replace(G5\_OPTION\_ID\_FILTER, '', trim(stripslashes($\_POST['opt2\_subject']))) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$opt3\_subject = isset($\_POST['opt3\_subject']) ? preg\_replace(G5\_OPTION\_ID\_FILTER, '', trim(stripslashes($\_POST['opt3\_subject']))) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$opt1\_val = isset($\_POST['opt1']) ? preg\_replace(G5\_OPTION\_ID\_FILTER, '', trim(stripslashes($\_POST['opt1']))) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$opt2\_val = isset($\_POST['opt2']) ? preg\_replace(G5\_OPTION\_ID\_FILTER, '', trim(stripslashes($\_POST['opt2']))) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$opt3\_val = isset($\_POST['opt3']) ? preg\_replace(G5\_OPTION\_ID\_FILTER, '', trim(stripslashes($\_POST['opt3']))) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="opt\_id[]" value="<?php echo $opt\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="opt\_chk\_<?php echo $i; ?>" class="sound\_only"></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="opt\_chk[]" id="opt\_chk\_<?php echo $i; ?>" value="1">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="opt-cell"><?php echo $opt\_1; if ($opt\_2\_len) echo ' <small>&gt;</small> '.$opt\_2; if ($opt\_3\_len) echo ' <small>&gt;</small> '.$opt\_3; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="opt\_price\_<?php echo $i; ?>" class="sound\_only"></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="opt\_price[]" value="<?php echo $opt\_price; ?>" id="opt\_price\_<?php echo $i; ?>" class="frm\_input" size="9">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="opt\_stock\_qty\_<?php echo $i; ?>" class="sound\_only"></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="opt\_stock\_qty[]" value="<?php echo $opt\_stock\_qty; ?>" id="op\_stock\_qty\_<?php echo $i; ?>" class="frm\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="opt\_noti\_qty\_<?php echo $i; ?>" class="sound\_only"></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="opt\_noti\_qty[]" value="<?php echo $opt\_noti\_qty; ?>" id="opt\_noti\_qty\_<?php echo $i; ?>" class="frm\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="opt\_use\_<?php echo $i; ?>" class="sound\_only"></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="opt\_use[]" id="opt\_use\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected('1', $opt\_use); ?>>사용함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected('0', $opt\_use); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 160 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="opt\_id[]" value="<?php echo $opt\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="opt\_chk\_<?php echo $i; ?>" class="sound\_only"></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="opt\_chk[]" id="opt\_chk\_<?php echo $i; ?>" value="1">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="opt1-cell"><?php echo $opt\_1; if ($opt\_2\_len) echo ' <small>&gt;</small> '.$opt\_2; if ($opt\_3\_len) echo ' <small>&gt;</small> '.$opt\_3; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="opt\_price\_<?php echo $i; ?>" class="sound\_only"></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="opt\_price[]" value="<?php echo $opt\_price; ?>" id="opt\_price\_<?php echo $i; ?>" class="frm\_input" size="9">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="opt\_stock\_qty\_<?php echo $i; ?>" class="sound\_only"></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="opt\_stock\_qty[]" value="<?php echo $opt\_stock\_qty; ?>" id="opt\_stock\_qty\_<?php echo $i; ?>" class="frm\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 174 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="opt\_noti\_qty\_<?php echo $i; ?>" class="sound\_only"></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 175 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="opt\_noti\_qty[]" value="<?php echo $opt\_noti\_qty; ?>" id="opt\_noti\_qty\_<?php echo $i; ?>" class="frm\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="opt\_use\_<?php echo $i; ?>" class="sound\_only"></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="opt\_use[]" id="opt\_use\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected('1', $opt\_use); ?>>사용함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 181 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected('0', $opt\_use); ?>>사용안함</option>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$iq\_id = isset($\_REQUEST['iq\_id']) ? preg\_replace('/[^0-9]/', '', $\_REQUEST['iq\_id']) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="iq\_id" value="<?php echo $iq\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 수정</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($iq['iq\_email']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo hyphen\_hp\_number($iq['iq\_hp']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="iq\_subject" value="<?php echo conv\_subject($iq['iq\_subject'],120); ?>" id="iq\_subject" required class="frm\_input required" size="95"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo editor\_html('iq\_question', get\_text(html\_purifier($iq['iq\_question']), 0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo editor\_html('iq\_answer', get\_text(html\_purifier($iq['iq\_answer']), 0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <td><textarea name="iq\_answer" id="iq\_answer" rows="7"><?php echo get\_text($iq['iq\_answer']); ?></textarea></td> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./itemqalist.php?<?php echo $qstr; ?>" class="btn btn\_02">목록</a>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace('/[^0-9]/', '', $default['de\_admin\_company\_tel']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqaformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$recv\_number = preg\_replace('/[^0-9]/', '', $row['iq\_hp']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt"> 전체 문의내역</span><span class="ov\_num"> <?php echo $total\_count; ?>건</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="save\_stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<option value="'.$row1['ca\_id'].'"'.$selected.'>'.$nbsp.$row1['ca\_name'].'</option>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="it\_name" <?php echo get\_selected($sfl, 'it\_name'); ?>>상품명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.it\_id" <?php echo get\_selected($sfl, 'a.it\_id'); ?>>상품코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx; ?>" id="stx" required class="frm\_input required">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i; ?>" class="sound\_only"><?php echo get\_text($row['iq\_subject']) ?> 상품문의</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk[]" value="<?php echo $i ?>" id="chk\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="iq\_id[<?php echo $i; ?>]" value="<?php echo $row['iq\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><a href="<?php echo $href; ?>"><?php echo get\_it\_image($row['it\_id'], 50, 50); ?> <?php echo cut\_str($row['it\_name'],30); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="#" class="qa\_href" onclick="return false;" target="<?php echo $i; ?>"><?php echo get\_text($row['iq\_subject']); ?> <span class="tit\_op">열기</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="qa\_div<?php echo $i; ?>" class="qa\_div" style="display:none;">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $iq\_question; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $iq\_answer; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_name"><?php echo $name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_boolean"><?php echo $answer; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./itemqaform.php?w=u&amp;iq\_id=<?php echo $row['iq\_id']; ?>&amp;<?php echo $qstr; ?>" class="btn btn\_03"><span class="sound\_only"><?php echo get\_text($row['iq\_subject']); ?> </span>수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3", $fr\_date);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3", $to\_date);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">등록상품 </span><span class="ov\_num"> <?php echo $total\_count; ?>건 </span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="doc" value="<?php echo $doc; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort1" value="<?php echo $sort1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort2" value="<?php echo $sort2; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<option value="'.$row1['ca\_id'].'" '.get\_selected($sel\_ca\_id, $row1['ca\_id']).'>'.$nbsp.$row1['ca\_name'].'</option>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="fr\_date" value="<?php echo $fr\_date; ?>" id="fr\_date" required class="required frm\_input" size="8" maxlength="8"> 에서

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="to\_date" value="<?php echo $to\_date; ?>" id="to\_date" required class="required frm\_input" size="8" maxlength="8"> 까지

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("ct\_status\_1",1)."&amp;$qstr1"; ?>">쇼핑</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("ct\_status\_2",1)."&amp;$qstr1"; ?>">주문</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("ct\_status\_3",1)."&amp;$qstr1"; ?>">입금</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("ct\_status\_4",1)."&amp;$qstr1"; ?>">준비</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("ct\_status\_5",1)."&amp;$qstr1"; ?>">배송</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("ct\_status\_6",1)."&amp;$qstr1"; ?>">완료</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("ct\_status\_7",1)."&amp;$qstr1"; ?>">취소</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("ct\_status\_8",1)."&amp;$qstr1"; ?>">반품</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("ct\_status\_9",1)."&amp;$qstr1"; ?>">품절</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("ct\_status\_sum",1)."&amp;$qstr1"; ?>">합계</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $num; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><a href="<?php echo $href; ?>"><?php echo get\_it\_image($row['it\_id'], 50, 50); ?> <?php echo cut\_str($row['it\_name'],30); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['ct\_status\_1']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['ct\_status\_2']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['ct\_status\_3']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['ct\_status\_4']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['ct\_status\_5']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['ct\_status\_6']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['ct\_status\_7']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['ct\_status\_8']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['ct\_status\_9']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['ct\_status\_sum']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsellrank.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr1&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">전체 상품</span><span class="ov\_num"> <?php echo $total\_count; ?>개</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="doc" value="<?php echo $doc; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort1" value="<?php echo $sort1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort2" value="<?php echo $sort2; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<option value="'.$row1['ca\_id'].'" '.get\_selected($sel\_ca\_id, $row1['ca\_id']).'>'.$nbsp.$row1['ca\_name'].'</option>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="it\_name" <?php echo get\_selected($sel\_field, 'it\_name'); ?>>상품명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="it\_id" <?php echo get\_selected($sel\_field, 'it\_id'); ?>>상품코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="search" id="search" value="<?php echo $search; ?>" required class="frm\_input required">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort1" value="<?php echo $sort1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort2" value="<?php echo $sort2; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sel\_ca\_id" value="<?php echo $sel\_ca\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sel\_field" value="<?php echo $sel\_field; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="search" value="<?php echo $search; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("it\_id") . "&amp;$qstr1"; ?>">상품코드</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("it\_name") . "&amp;$qstr1"; ?>">상품명</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("it\_stock\_qty") . "&amp;$qstr1"; ?>">창고재고</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("it\_use") . "&amp;$qstr1"; ?>">판매</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("it\_soldout") . "&amp;$qstr1"; ?>">품절</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("it\_stock\_sms") . "&amp;$qstr1"; ?>">재입고알림</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[<?php echo $i; ?>]" value="<?php echo $row['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $row['it\_id']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><a href="<?php echo $href; ?>"><?php echo get\_it\_image($row['it\_id'], 50, 50); ?> <?php echo cut\_str(stripslashes($row['it\_name']), 60, "&#133"); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 174 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num<?php echo $it\_stock\_qty\_st; ?>"><?php echo $it\_stock\_qty; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 175 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($wait\_qty); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($temporary\_qty); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="stock\_qty\_<?php echo $i; ?>" class="sound\_only">재고수정</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_stock\_qty[<?php echo $i; ?>]" value="<?php echo $row['it\_stock\_qty']; ?>" id="stock\_qty\_<?php echo $i; ?>" class="frm\_input" size="10" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 182 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="noti\_qty\_<?php echo $i; ?>" class="sound\_only">통보수량</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 183 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="it\_noti\_qty[<?php echo $i; ?>]" value="<?php echo $row['it\_noti\_qty']; ?>" id="noti\_qty\_<?php echo $i; ?>" class="frm\_input" size="10" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 186 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="use\_<?php echo $i; ?>" class="sound\_only">판매</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_use[<?php echo $i; ?>]" value="1" id="use\_<?php echo $i; ?>" <?php echo ($row['it\_use'] ? "checked" : ""); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 190 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="soldout\_<?php echo $i; ?>" class="sound\_only">품절</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 191 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_soldout[<?php echo $i; ?>]" value="1" id="soldout\_<?php echo $i; ?>" <?php echo ($row['it\_soldout'] ? "checked" : ""); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 194 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="stock\_sms\_<?php echo $i; ?>" class="sound\_only">재입고 알림</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_stock\_sms[<?php echo $i; ?>]" value="1" id="stock\_sms\_<?php echo $i; ?>" <?php echo ($row['it\_stock\_sms'] ? "checked" : ""); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 197 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mng td\_mng\_s"><a href="./itemform.php?w=u&amp;it\_id=<?php echo $row['it\_id']; ?>&amp;ca\_id=<?php echo $row['ca\_id']; ?>&amp;<?php echo $qstr; ?>" class="btn btn\_03">수정</a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 215 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['g5\_shop\_item\_stocksms\_table']}` (

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">전체 </span><span class="ov\_num"> <?php echo number\_format($total\_count); ?>건</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">미전송 </span><span class="ov\_num"><?php echo number\_format($unsend\_count); ?>건</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="doc" value="<?php echo $doc; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort1" value="<?php echo $sort1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort2" value="<?php echo $sort2; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="it\_id" <?php echo get\_selected($sel\_field, 'it\_id'); ?>>상품코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="ss\_hp" <?php echo get\_selected($sel\_field, 'ss\_hp'); ?>>휴대폰번호</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="search" id="search" value="<?php echo $search; ?>" required class="frm\_input required">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort1" value="<?php echo $sort1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort2" value="<?php echo $sort2; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sel\_field" value="<?php echo $sel\_field; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="search" value="<?php echo $search; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i; ?>" class="sound\_only"><?php echo $it\_name; ?> 알림요청</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk[]" value="<?php echo $i ?>" id="chk\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ss\_id[<?php echo $i; ?>]" value="<?php echo $row['ss\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><?php echo $it\_name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_telbig"><?php echo $row['ss\_hp']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_stat"><?php echo ($row['ss\_send'] ? '전송완료' : '전송전'); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo (is\_null\_time($row['ss\_send\_time']) ? '' : $row['ss\_send\_time']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo (is\_null\_time($row['ss\_datetime']) ? '' : $row['ss\_datetime']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksmsupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$receive\_number = preg\_replace("/[^0-9]/", "", $row['ss\_hp']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemstocksmsupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace("/[^0-9]/", "", $default['de\_admin\_company\_tel']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spl\_id[]" value="<?php echo $spl\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="spl\_chk\_<?php echo $i; ?>" class="sound\_only"><?php echo $spl\_subject.' '.$spl; ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="spl\_chk[]" id="spl\_chk\_<?php echo $i; ?>" value="1">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="spl-subject-cell"><?php echo $spl\_subject; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="spl-cell"><?php echo $spl; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="spl\_price\_<?php echo $i; ?>" class="sound\_only">상품금액</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="spl\_price[]" value="<?php echo $spl\_price; ?>" id="spl\_price\_<?php echo $i; ?>" class="frm\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="spl\_stock\_qty\_<?php echo $i; ?>" class="sound\_only">재고수량</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="spl\_stock\_qty[]" value="<?php echo $spl\_stock\_qty; ?>" id="spl\_stock\_qty\_<?php echo $i; ?>" class="frm\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="spl\_noti\_qty\_<?php echo $i; ?>" class="sound\_only">통보수량</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="spl\_noti\_qty[]" value="<?php echo $spl\_noti\_qty; ?>" id="spl\_noti\_qty\_<?php echo $i; ?>" class="frm\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="spl\_use\_<?php echo $i; ?>" class="sound\_only">사용여부</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="spl\_use[]" id="spl\_use\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected('1', $spl\_use); ?>>사용함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected('0', $spl\_use); ?>>사용안함</option>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$spl\_subject = isset($\_POST['subject'][$i]) ? preg\_replace(G5\_OPTION\_ID\_FILTER, '', trim(stripslashes($\_POST['subject'][$i]))) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$spl\_val = isset($\_POST['supply'][$i]) ? explode(',', preg\_replace(G5\_OPTION\_ID\_FILTER, '', trim(stripslashes($\_POST['supply'][$i])))) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spl\_id[]" value="<?php echo $spl\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="spl\_chk\_<?php echo $i; ?>" class="sound\_only"><?php echo $spl\_subject.' '.$spl; ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="spl\_chk[]" id="spl\_chk\_<?php echo $i; ?>" value="1">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="spl-subject-cell"><?php echo $spl\_subject; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="spl-cell"><?php echo $spl; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="spl\_price\_<?php echo $i; ?>" class="sound\_only">상품금액</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="spl\_price[]" value="<?php echo $spl\_price; ?>" id="spl\_price\_<?php echo $i; ?>" class="frm\_input" size="9">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="spl\_stock\_qty\_<?php echo $i; ?>" class="sound\_only">재고수량</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="spl\_stock\_qty[]" value="<?php echo $spl\_stock\_qty; ?>" id="spl\_stock\_qty\_<?php echo $i; ?>" class="frm\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="spl\_noti\_qty\_<?php echo $i; ?>" class="sound\_only">통보수량</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="spl\_noti\_qty[]" value="<?php echo $spl\_noti\_qty; ?>" id="spl\_noti\_qty\_<?php echo $i; ?>" class="frm\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="spl\_use\_<?php echo $i; ?>" class="sound\_only">사용여부</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="spl\_use[]" id="spl\_use\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected('1', $spl\_use); ?>>사용함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemsupply.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected('0', $spl\_use); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">전체 상품</span><span class="ov\_num"> <?php echo $total\_count; ?>개</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="doc" value="<?php echo $doc; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<option value="'.$row1['ca\_id'].'" '.get\_selected($sca, $row1['ca\_id']).'>'.$nbsp.$row1['ca\_name'].PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="it\_name" <?php echo get\_selected($sfl, 'it\_name'); ?>>상품명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="it\_id" <?php echo get\_selected($sfl, 'it\_id'); ?>>상품코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx; ?>" id="stx" required class="frm\_input required">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><?php echo subject\_sort\_link("it\_id", $qstr, 1); ?>상품코드</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><?php echo subject\_sort\_link("it\_type1", $qstr, 1); ?>히트<br>상품</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><?php echo subject\_sort\_link("it\_type2", $qstr, 1); ?>추천<br>상품</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><?php echo subject\_sort\_link("it\_type3", $qstr, 1); ?>신규<br>상품</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><?php echo subject\_sort\_link("it\_type4", $qstr, 1); ?>인기<br>상품</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><?php echo subject\_sort\_link("it\_type5", $qstr, 1); ?>할인<br>상품</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[<?php echo $i; ?>]" value="<?php echo $row['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $row['it\_id']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><a href="<?php echo $href; ?>"><?php echo get\_it\_image($row['it\_id'], 50, 50); ?><?php echo cut\_str(stripslashes($row['it\_name']), 60, "&#133"); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="type1\_<?php echo $i; ?>" class="sound\_only">히트상품</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_type1[<?php echo $i; ?>]" value="1" id="type1\_<?php echo $i; ?>" <?php echo ($row['it\_type1'] ? 'checked' : ''); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="type2\_<?php echo $i; ?>" class="sound\_only">추천상품</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_type2[<?php echo $i; ?>]" value="1" id="type2\_<?php echo $i; ?>" <?php echo ($row['it\_type2'] ? 'checked' : ''); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="type3\_<?php echo $i; ?>" class="sound\_only">신규상품</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_type3[<?php echo $i; ?>]" value="1" id="type3\_<?php echo $i; ?>" <?php echo ($row['it\_type3'] ? 'checked' : ''); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="type4\_<?php echo $i; ?>" class="sound\_only">인기상품</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_type4[<?php echo $i; ?>]" value="1" id="type4\_<?php echo $i; ?>" <?php echo ($row['it\_type4'] ? 'checked' : ''); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="type5\_<?php echo $i; ?>" class="sound\_only">할인상품</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="it\_type5[<?php echo $i; ?>]" value="1" id="type5\_<?php echo $i; ?>" <?php echo ($row['it\_type5'] ? 'checked' : ''); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 174 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./itemform.php?w=u&amp;it\_id=<?php echo $row['it\_id']; ?>&amp;ca\_id=<?php echo $row['ca\_id']; ?>&amp;<?php echo $qstr; ?>" class="btn btn\_03"><span class="sound\_only"><?php echo cut\_str(stripslashes($row['it\_name']), 60, "&#133"); ?> </span>수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 192 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemtypelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$is\_id = isset($\_GET['is\_id']) ? preg\_replace('/[^0-9]/', '', $\_GET['is\_id']) : 0;

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_item\_use\_table']}`

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="is\_id" value="<?php echo $is\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id" value="<?php echo $is['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 수정</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><a href="<?php echo shop\_item\_url($is['it\_id']); ?>"><?php echo $is['it\_name']; ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><img src="<?php echo G5\_URL; ?>/shop/img/s\_star<?php echo $is['is\_score']; ?>.png" width="100"> (<?php echo $is['is\_score']; ?>점)</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

value="<?php echo get\_text($is['is\_subject']); ?>"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo editor\_html('is\_content', get\_text(html\_purifier($is['is\_content']), 0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

value="<?php echo get\_text($is['is\_reply\_subject']); ?>"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo editor\_html('is\_reply\_content', get\_text(html\_purifier($is['is\_reply\_content']), 0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_confirm" value="1" id="is\_confirm\_yes" <?php echo $is\_confirm\_yes; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_confirm" value="0" id="is\_confirm\_no" <?php echo $is\_confirm\_no; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./itemuselist.php?<?php echo $qstr; ?>" class="btn\_02 btn">목록</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt"> 전체 후기내역</span><span class="ov\_num"> <?php echo $total\_count; ?>건</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="save\_stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<option value="'.$row1['ca\_id'].'"'.$selected.'>'.$nbsp.$row1['ca\_name'].'</option>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="it\_name" <?php echo get\_selected($sfl, 'it\_name'); ?>>상품명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.it\_id" <?php echo get\_selected($sfl, 'a.it\_id'); ?>>상품코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="is\_name" <?php echo get\_selected($sfl, 'is\_name'); ?>>이름</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" id="stx" value="<?php echo $stx; ?>" required class="frm\_input required">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i; ?>" class="sound\_only"><?php echo get\_text($row['is\_subject']) ?> 사용후기</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk[]" value="<?php echo $i ?>" id="chk\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="is\_id[<?php echo $i; ?>]" value="<?php echo $row['is\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[<?php echo $i; ?>]" value="<?php echo $row['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><a href="<?php echo $href; ?>"><?php echo get\_it\_image($row['it\_id'], 50, 50); ?><?php echo cut\_str($row['it\_name'],30); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_name"><?php echo $name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="#" class="use\_href" onclick="return false;" target="<?php echo $i; ?>"><?php echo get\_text($row['is\_subject']); ?><span class="tit\_op">열기</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="use\_div<?php echo $i; ?>" class="use\_div" style="display:none;">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_content; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="score\_<?php echo $i; ?>" class="sound\_only">평점</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="is\_score[<?php echo $i; ?>]" id="score\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="5" <?php echo get\_selected($row['is\_score'], "5"); ?>>매우만족</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="4" <?php echo get\_selected($row['is\_score'], "4"); ?>>만족</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="3" <?php echo get\_selected($row['is\_score'], "3"); ?>>보통</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="2" <?php echo get\_selected($row['is\_score'], "2"); ?>>불만</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($row['is\_score'], "1"); ?>>매우불만</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="confirm\_<?php echo $i; ?>" class="sound\_only">확인</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 160 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="is\_confirm[<?php echo $i; ?>]" <?php echo ($row['is\_confirm'] ? 'checked' : ''); ?> value="1" id="confirm\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./itemuseform.php?w=u&amp;is\_id=<?php echo $row['is\_id']; ?>&amp;<?php echo $qstr; ?>" class="btn btn\_03"><span class="sound\_only"><?php echo get\_text($row['is\_subject']); ?> </span>수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 184 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\itemuselistupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$iit\_id = isset($\_POST['it\_id'][$k]) ? preg\_replace('/[^a-z0-9\_\-]/i', '', $\_POST['it\_id'][$k]) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">전체 옵션</span><span class="ov\_num"> <?php echo $total\_count; ?>개</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="doc" value="<?php echo $doc; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort1" value="<?php echo $sort1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort2" value="<?php echo $sort2; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<option value="'.$row1['ca\_id'].'" '.get\_selected($sel\_ca\_id, $row1['ca\_id']).'>'.$nbsp.$row1['ca\_name'].'</option>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="b.it\_name" <?php echo get\_selected($sel\_field, 'b.it\_name'); ?>>상품명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.it\_id" <?php echo get\_selected($sel\_field, 'a.it\_id'); ?>>상품코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="search" id="search" value="<?php echo $search; ?>" required class="frm\_input required">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort1" value="<?php echo $sort1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort2" value="<?php echo $sort2; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sel\_ca\_id" value="<?php echo $sel\_ca\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sel\_field" value="<?php echo $sel\_field; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="search" value="<?php echo $search; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("b.it\_name") . "&amp;$qstr1"; ?>">상품명</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("a.io\_stock\_qty") . "&amp;$qstr1"; ?>">창고재고</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><a href="<?php echo title\_sort("a.io\_use") . "&amp;$qstr1"; ?>">판매</a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[<?php echo $i; ?>]" value="<?php echo $row['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 181 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_id[<?php echo $i; ?>]" value="<?php echo $row['io\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 182 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_type[<?php echo $i; ?>]" value="<?php echo $row['io\_type']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 183 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $href; ?>"><?php echo get\_it\_image($row['it\_id'], 50, 50); ?> <?php echo cut\_str(stripslashes($row['it\_name']), 60, "&#133"); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 185 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><?php echo $option; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 186 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mng"><?php echo $type; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num<?php echo $io\_stock\_qty\_st; ?>"><?php echo $io\_stock\_qty; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($wait\_qty); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 189 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($temporary\_qty); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 191 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="stock\_qty\_<?php echo $i; ?>" class="sound\_only">재고수정</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 192 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="io\_stock\_qty[<?php echo $i; ?>]" value="<?php echo $row['io\_stock\_qty']; ?>" id="stock\_qty\_<?php echo $i; ?>" class="frm\_input" size="8" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="noti\_qty\_<?php echo $i; ?>" class="sound\_only">통보수량</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 196 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="io\_noti\_qty[<?php echo $i; ?>]" value="<?php echo $row['io\_noti\_qty']; ?>" id="noti\_qty\_<?php echo $i; ?>" class="frm\_input" size="8" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 199 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="use\_<?php echo $i; ?>" class="sound\_only">판매</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 200 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="io\_use[<?php echo $i; ?>]" value="1" id="use\_<?php echo $i; ?>" <?php echo ($row['io\_use'] ? "checked" : ""); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 202 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mng td\_mng\_s"><a href="./itemform.php?w=u&amp;it\_id=<?php echo $row['it\_id']; ?>&amp;ca\_id=<?php echo $row['ca\_id']; ?>&amp;<?php echo $qstr; ?>" class="btn btn\_03">수정</a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 228 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\optionstocklistupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$io\_id = isset($\_POST['io\_id'][$i]) ? preg\_replace(G5\_OPTION\_ID\_FILTER, '', $\_POST['io\_id'][$i]) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderdelivery.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title']; ?></h1>

**STANDARD: Potentially Unsafe Code - fopen**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderdeliveryexcel.php

$fh=fopen($fname, "rb");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderdeliveryexcel.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fh=fopen($fname, "rb");

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderdeliveryupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$receive\_number = preg\_replace("/[^0-9]/", "", $od['od\_hp']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderdeliveryupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace("/[^0-9]/", "", $default['de\_admin\_company\_tel']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderdeliveryupdate.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title']; ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderdeliveryupdate.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo number\_format($total\_count); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderdeliveryupdate.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="result\_done"><?php echo number\_format($succ\_count); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderdeliveryupdate.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="result\_fail"><?php echo number\_format($fail\_count); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderdeliveryupdate.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo implode(', ', $fail\_od\_id); ?></dd>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr\_date = isset($\_REQUEST['fr\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['fr\_date']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to\_date = isset($\_REQUEST['to\_date']) ? preg\_replace('/[^0-9 :\-]/i', '', $\_REQUEST['to\_date']) : '';

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_order\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_order\_address\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_order\_table']}`

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

현재 주문상태 <strong><?php echo $od['od\_status'] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

주문일시 <strong><?php echo substr($od['od\_time'],0,16); ?> (<?php echo get\_yoil($od['od\_time']); ?>)</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

주문총액 <strong><?php echo number\_format($od['od\_cart\_price'] + $od['od\_send\_cost'] + $od['od\_send\_cost2']); ?></strong>원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($default['de\_hope\_date\_use']) { ?><p>희망배송일은 <?php echo $od['od\_hope\_date']; ?> (<?php echo get\_yoil($od['od\_hope\_date']); ?>) 입니다.</p><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_id" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $od['mb\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_email" value="<?php echo $od['od\_email']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort1" value="<?php echo $sort1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort2" value="<?php echo $sort2; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sel\_field" value="<?php echo $sel\_field; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="search" value="<?php echo $search; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page;?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 222 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td rowspan="<?php echo $rowspan; ?>" class="td\_left">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 223 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./itemform.php?w=u&amp;it\_id=<?php echo $row['it\_id']; ?>"><?php echo $image; ?> <?php echo stripslashes($row['it\_name']); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 224 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($od['od\_tax\_flag'] && $row['ct\_notax']) echo '[비과세상품]'; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 226 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td rowspan="<?php echo $rowspan; ?>" class="td\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 227 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="sit\_sel\_<?php echo $i; ?>" class="sound\_only"><?php echo $row['it\_name']; ?> 옵션 전체선택</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 228 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="sit\_sel\_<?php echo $i; ?>" name="it\_sel[]">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 232 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ct\_chk\_<?php echo $chk\_cnt; ?>" class="sound\_only"><?php echo get\_text($opt['ct\_option']); ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 233 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="ct\_chk[<?php echo $chk\_cnt; ?>]" id="ct\_chk\_<?php echo $chk\_cnt; ?>" value="<?php echo $chk\_cnt; ?>" class="sct\_sel\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 234 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ct\_id[<?php echo $chk\_cnt; ?>]" value="<?php echo $opt['ct\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 235 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_text($opt['ct\_option']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 237 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mngsmall"><?php echo $opt['ct\_status']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 239 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ct\_qty\_<?php echo $chk\_cnt; ?>" class="sound\_only"><?php echo get\_text($opt['ct\_option']); ?> 수량</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 240 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ct\_qty[<?php echo $chk\_cnt; ?>]" id="ct\_qty\_<?php echo $chk\_cnt; ?>" value="<?php echo $opt['ct\_qty']; ?>" required class="frm\_input required" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 242 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right "><?php echo number\_format($opt\_price); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 243 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($ct\_price['stotal']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 244 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($opt['cp\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 245 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class=" td\_num\_right"><?php echo number\_format($ct\_point['stotal']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 246 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_sendcost\_by"><?php echo $ct\_send\_cost; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 247 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mngsmall"><?php echo get\_yn($opt['ct\_point\_use']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 248 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mngsmall"><?php echo get\_yn($opt['ct\_stock\_use']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 263 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="chk\_cnt" value="<?php echo $chk\_cnt; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 287 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($od['od\_mod\_history'], 0); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 310 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 336 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="sodr\_nonpay">미수금 <?php echo display\_price($od['od\_misu']); ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 354 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od['od\_id']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 355 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_paybybig"><?php echo $s\_receipt\_way; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 356 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig td\_numsum"><?php echo display\_price($amount['order']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 357 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig"><?php echo display\_price($od['od\_send\_cost'] + $od['od\_send\_cost2']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 358 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig"><?php echo display\_point($od['od\_receipt\_point']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 359 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig td\_numincome"><?php echo number\_format($amount['receipt']); ?>원</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 360 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig td\_numcoupon"><?php echo display\_price($amount['coupon']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 361 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig td\_numcancel"><?php echo number\_format($amount['cancel']); ?>원</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 370 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 373 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_id" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 374 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort1" value="<?php echo $sort1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 375 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort2" value="<?php echo $sort2; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 376 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sel\_field" value="<?php echo $sel\_field; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 377 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="search" value="<?php echo $search; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 378 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 379 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_name" value="<?php echo $od['od\_name']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 380 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_hp" value="<?php echo $od['od\_hp']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 381 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_tno" value="<?php echo $od['od\_tno']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 382 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_escrow" value="<?php echo $od['od\_escrow']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 383 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_pg" value="<?php echo $od['od\_pg']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 402 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_bank\_account']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 406 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><?php echo $od['od\_settle\_case']; ?> 입금액</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 407 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_price($od['od\_receipt\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 411 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_deposit\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 417 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php } else { ?><?php echo $od['od\_receipt\_time']; ?> (<?php echo get\_yoil($od['od\_receipt\_time']); ?>)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 426 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_bank\_account']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 429 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><?php echo $od['od\_settle\_case']; ?> 결제액</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 430 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_price($od['od\_receipt\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 436 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php } else { ?><?php echo $od['od\_receipt\_time']; ?> (<?php echo get\_yoil($od['od\_receipt\_time']); ?>)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 447 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php } else { ?><?php echo display\_price($od['od\_receipt\_price']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 455 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php } else { ?><?php echo substr($od['od\_receipt\_time'], 0, 20); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 466 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php } else { ?><?php echo display\_price($od['od\_receipt\_price']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 474 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php } else { ?><?php echo substr($od['od\_receipt\_time'], 0, 20); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 482 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" class="sodr\_sppay"><?php echo $s\_receipt\_way; ?> 결제금액</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 485 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php } else { ?><?php echo display\_price($od['od\_receipt\_price']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 490 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" class="sodr\_sppay"><?php echo $s\_receipt\_way; ?> 승인일시</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 492 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($od['od\_receipt\_time'] == "0000-00-00 00:00:00") { echo $s\_receipt\_way; ?> 결제 일시 정보가 없습니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 493 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php } else { ?><?php echo substr($od['od\_receipt\_time'], 0, 20); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 534 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"{$pg\_url}\" target=\"\_blank\">{$pg\_test}바로가기</a><br>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 545 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_price($od['od\_tax\_mny']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 549 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_price($od['od\_vat\_mny']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 553 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_price($od['od\_free\_mny']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 558 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_price($od['od\_coupon']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 562 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_point($od['od\_receipt\_point']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 566 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_price($od['od\_refund\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 571 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od['od\_delivery\_company']; ?> <?php echo get\_delivery\_inquiry($od['od\_delivery\_company'], $od['od\_invoice'], 'dvr\_link'); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 575 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od['od\_invoice']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 579 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo is\_null\_time($od['od\_invoice\_time']) ? "" : $od['od\_invoice\_time']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 585 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_send\_cost" value="<?php echo $od['od\_send\_cost']; ?>" id="od\_send\_cost" class="frm\_input" size="10"> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 591 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_price($od['od\_send\_coupon']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 597 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_send\_cost2" value="<?php echo $od['od\_send\_cost2']; ?>" id="od\_send\_cost2" class="frm\_input" size="10"> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 633 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $cash\_receipt\_script; ?>">현금영수증 확인</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 635 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="window.open('<?php echo G5\_SHOP\_URL; ?>/taxsave.php?od\_id=<?php echo $od\_id; ?>', 'taxsave', 'width=550,height=400,scrollbars=1,menus=0');">현금영수증 발급</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 681 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $bank\_account; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 686 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><label for="od\_receipt\_price"><?php echo $od['od\_settle\_case']; ?> 입금액</label></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 688 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $html\_receipt\_chk; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 689 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_receipt\_price" value="<?php echo $od['od\_receipt\_price']; ?>" id="od\_receipt\_price" class="frm\_input"> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 700 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_deposit\_name" value="<?php echo get\_text($od['od\_deposit\_name']); ?>" id="od\_deposit\_name" class="frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 708 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_receipt\_time" value="<?php echo is\_null\_time($od['od\_receipt\_time']) ? "" : $od['od\_receipt\_time']; ?>" id="od\_receipt\_time" class="frm\_input" maxlength="19">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 716 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_bank\_account']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 719 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><label for="od\_receipt\_price"><?php echo $od['od\_settle\_case']; ?> 결제액</label></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 721 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $html\_receipt\_chk; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 722 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_receipt\_price" value="<?php echo $od['od\_receipt\_price']; ?>" id="od\_receipt\_price" class="frm\_input"> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 730 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_receipt\_time" value="<?php echo is\_null\_time($od['od\_receipt\_time']) ? "" : $od['od\_receipt\_time']; ?>" id="op\_receipt\_time" class="frm\_input" size="19" maxlength="19">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 739 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $html\_receipt\_chk; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 740 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_receipt\_price" id="od\_receipt\_price" value="<?php echo $od['od\_receipt\_price']; ?>" class="frm\_input" size="10"> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 748 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_receipt\_time" value="<?php echo is\_null\_time($od['od\_receipt\_time']) ? "" : $od['od\_receipt\_time']; ?>" id="od\_receipt\_time" class="frm\_input" size="19" maxlength="19">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 757 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $html\_receipt\_chk; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 758 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_receipt\_price" id="od\_receipt\_price" value="<?php echo $od['od\_receipt\_price']; ?>" class="frm\_input" size="10"> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 766 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_receipt\_time" value="<?php echo is\_null\_time($od['od\_receipt\_time']) ? "" : $od['od\_receipt\_time']; ?>" id="od\_receipt\_time" class="frm\_input" size="19" maxlength="19">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 773 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" class="sodr\_sppay"><label for="od\_receipt\_price"><?php echo $s\_receipt\_way; ?> 결제금액</label></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 775 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $html\_receipt\_chk; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 776 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_receipt\_price" id="od\_receipt\_price" value="<?php echo $od['od\_receipt\_price']; ?>" class="frm\_input" size="10"> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 780 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" class="sodr\_sppay"><label for="od\_receipt\_time"><?php echo $s\_receipt\_way; ?> 승인일시</label></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 784 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_receipt\_time" value="<?php echo is\_null\_time($od['od\_receipt\_time']) ? "" : $od['od\_receipt\_time']; ?>" id="od\_receipt\_time" class="frm\_input" size="19" maxlength="19">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 791 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="od\_receipt\_point" value="<?php echo $od['od\_receipt\_point']; ?>" id="od\_receipt\_point" class="frm\_input" size="10"> 점</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 796 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_refund\_price" value="<?php echo $od['od\_refund\_price']; ?>" id="od\_refund\_price" class="frm\_input" size="10"> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 807 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_invoice" value="<?php echo $od['od\_invoice']; ?>" id="od\_invoice" class="frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 813 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="od\_delivery\_chk" value="<?php echo $default['de\_delivery\_company']; ?>" onclick="chk\_delivery\_company()">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 815 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_delivery\_company" id="od\_delivery\_company" value="<?php echo $od['od\_delivery\_company']; ?>" class="frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 823 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_invoice\_time" id="od\_invoice\_time" value="<?php echo is\_null\_time($od['od\_invoice\_time']) ? "" : $od['od\_invoice\_time']; ?>" class="frm\_input" maxlength="19">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 847 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./personalpayform.php?popup=yes&amp;od\_id=<?php echo $od\_id; ?>" id="personalpay\_add" class="btn btn\_02">개인결제추가</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 850 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./orderpartcancel.php?od\_id=<?php echo $od\_id; ?>" id="orderpartcancel" class="btn btn\_02"><?php echo $od['od\_settle\_case']; ?> 부분취소</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 852 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./orderlist.php?<?php echo $qstr; ?>" class="btn btn\_02">목록</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 859 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 868 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_id" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 869 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort1" value="<?php echo $sort1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 870 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort2" value="<?php echo $sort2; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 871 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sel\_field" value="<?php echo $sel\_field; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 872 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="search" value="<?php echo $search; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 873 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 878 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="od\_shop\_memo" id="od\_shop\_memo" rows="8"><?php echo html\_purifier(stripslashes($od['od\_shop\_memo'])); ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 890 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 893 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_id" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 894 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort1" value="<?php echo $sort1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 895 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort2" value="<?php echo $sort2; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 896 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sel\_field" value="<?php echo $sel\_field; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 897 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="search" value="<?php echo $search; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 898 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 916 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="od\_name" value="<?php echo get\_text($od['od\_name']); ?>" id="od\_name" required class="frm\_input required"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 920 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="od\_tel" value="<?php echo get\_text($od['od\_tel']); ?>" id="od\_tel" required class="frm\_input required"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 924 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="od\_hp" value="<?php echo get\_text($od['od\_hp']); ?>" id="od\_hp" class="frm\_input"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 930 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_zip" value="<?php echo get\_text($od['od\_zip1']).get\_text($od['od\_zip2']); ?>" id="od\_zip" required class="frm\_input required" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 933 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_addr1" value="<?php echo get\_text($od['od\_addr1']); ?>" id="od\_addr1" required class="frm\_input required" size="35">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 935 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_addr2" value="<?php echo get\_text($od['od\_addr2']); ?>" id="od\_addr2" class="frm\_input" size="35">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 938 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_addr3" value="<?php echo get\_text($od['od\_addr3']); ?>" id="od\_addr3" class="frm\_input" size="35">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 940 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_addr\_jibeon" value="<?php echo get\_text($od['od\_addr\_jibeon']); ?>"><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 945 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="od\_email" value="<?php echo $od['od\_email']; ?>" id="od\_email" required class="frm\_input required" size="30"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 949 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od['od\_ip']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 969 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="od\_b\_name" value="<?php echo get\_text($od['od\_b\_name']); ?>" id="od\_b\_name" required class="frm\_input required"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 973 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="od\_b\_tel" value="<?php echo get\_text($od['od\_b\_tel']); ?>" id="od\_b\_tel" required class="frm\_input required"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 977 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="od\_b\_hp" value="<?php echo get\_text($od['od\_b\_hp']); ?>" id="od\_b\_hp" class="frm\_input required"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 983 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_b\_zip" value="<?php echo get\_text($od['od\_b\_zip1']).get\_text($od['od\_b\_zip2']); ?>" id="od\_b\_zip" required class="frm\_input required" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 985 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_b\_addr1" value="<?php echo get\_text($od['od\_b\_addr1']); ?>" id="od\_b\_addr1" required class="frm\_input required" size="35">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 987 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_b\_addr2" value="<?php echo get\_text($od['od\_b\_addr2']); ?>" id="od\_b\_addr2" class="frm\_input" size="35">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 989 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_b\_addr3" value="<?php echo get\_text($od['od\_b\_addr3']); ?>" id="od\_b\_addr3" class="frm\_input" size="35">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 991 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_b\_addr\_jibeon" value="<?php echo get\_text($od['od\_b\_addr\_jibeon']); ?>"><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 999 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_hope\_date" value="<?php echo $od['od\_hope\_date']; ?>" id="od\_hopedate" required class="frm\_input required" maxlength="10" minlength="10"> (<?php echo get\_yoil($od['od\_hope\_date']); ?>)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1006 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php if ($od['od\_memo']) echo get\_text($od['od\_memo'], 1);else echo "없음";?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1017 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./orderlist.php?<?php echo $qstr; ?>" class="btn">목록</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1086 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var cancel\_pg = "PG사의 <?php echo $od['od\_settle\_case']; ?>";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_zip1 = isset($\_POST['od\_zip']) ? preg\_replace('/[^0-9]/', '', substr($\_POST['od\_zip'], 0, 3)) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_zip2 = isset($\_POST['od\_zip']) ? preg\_replace('/[^0-9]/', '', substr($\_POST['od\_zip'], 3)) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_b\_zip1 = isset($\_POST['od\_b\_zip']) ? preg\_replace('/[^0-9]/', '', substr($\_POST['od\_b\_zip'], 0, 3)) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_b\_zip2 = isset($\_POST['od\_b\_zip']) ? preg\_replace('/[^0-9]/', '', substr($\_POST['od\_b\_zip'], 3)) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_misu = isset($\_GET['od\_misu']) ? preg\_replace('/[^0-9a-z]/i', '', $\_GET['od\_misu']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_cancel\_price = isset($\_GET['od\_cancel\_price']) ? preg\_replace('/[^0-9a-z]/', '', $\_GET['od\_cancel\_price']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_refund\_price = isset($\_GET['od\_refund\_price']) ? preg\_replace('/[^0-9a-z]/i', '', $\_GET['od\_refund\_price']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_receipt\_point = isset($\_GET['od\_receipt\_point']) ? preg\_replace('/[^0-9a-z]/i', '', $\_GET['od\_receipt\_point']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_coupon = isset($\_GET['od\_coupon']) ? preg\_replace('/[^0-9a-z]/i', '', $\_GET['od\_coupon']) : '';

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_order\_delete\_table']}`

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">전체 주문내역</span><span class="ov\_num"> <?php echo number\_format($total\_count); ?>건</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="doc" value="<?php echo $doc; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort1" value="<?php echo $sort1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sort2" value="<?php echo $sort2; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="save\_search" value="<?php echo $search; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="od\_id" <?php echo get\_selected($sel\_field, 'od\_id'); ?>>주문번호</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 172 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mb\_id" <?php echo get\_selected($sel\_field, 'mb\_id'); ?>>회원 ID</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="od\_name" <?php echo get\_selected($sel\_field, 'od\_name'); ?>>주문자</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 174 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="od\_tel" <?php echo get\_selected($sel\_field, 'od\_tel'); ?>>주문자전화</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 175 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="od\_hp" <?php echo get\_selected($sel\_field, 'od\_hp'); ?>>주문자핸드폰</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="od\_b\_name" <?php echo get\_selected($sel\_field, 'od\_b\_name'); ?>>받는분</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="od\_b\_tel" <?php echo get\_selected($sel\_field, 'od\_b\_tel'); ?>>받는분전화</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="od\_b\_hp" <?php echo get\_selected($sel\_field, 'od\_b\_hp'); ?>>받는분핸드폰</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="od\_deposit\_name" <?php echo get\_selected($sel\_field, 'od\_deposit\_name'); ?>>입금자</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="od\_invoice" <?php echo get\_selected($sel\_field, 'od\_invoice'); ?>>운송장번호</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 184 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="search" value="<?php echo $search; ?>" id="search" required class="required frm\_input" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 192 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="od\_status" value="" id="od\_status\_all" <?php echo get\_checked($od\_status, ''); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 194 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="od\_status" value="주문" id="od\_status\_odr" <?php echo get\_checked($od\_status, '주문'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 196 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="od\_status" value="입금" id="od\_status\_income" <?php echo get\_checked($od\_status, '입금'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 198 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="od\_status" value="준비" id="od\_status\_rdy" <?php echo get\_checked($od\_status, '준비'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 200 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="od\_status" value="배송" id="od\_status\_dvr" <?php echo get\_checked($od\_status, '배송'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 202 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="od\_status" value="완료" id="od\_status\_done" <?php echo get\_checked($od\_status, '완료'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 204 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="od\_status" value="전체취소" id="od\_status\_cancel" <?php echo get\_checked($od\_status, '전체취소'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 206 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="od\_status" value="부분취소" id="od\_status\_pcancel" <?php echo get\_checked($od\_status, '부분취소'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 212 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="od\_settle\_case" value="" id="od\_settle\_case01" <?php echo get\_checked($od\_settle\_case, ''); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 214 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="od\_settle\_case" value="무통장" id="od\_settle\_case02" <?php echo get\_checked($od\_settle\_case, '무통장'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 216 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="od\_settle\_case" value="가상계좌" id="od\_settle\_case03" <?php echo get\_checked($od\_settle\_case, '가상계좌'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 218 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="od\_settle\_case" value="계좌이체" id="od\_settle\_case04" <?php echo get\_checked($od\_settle\_case, '계좌이체'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 220 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="od\_settle\_case" value="휴대폰" id="od\_settle\_case05" <?php echo get\_checked($od\_settle\_case, '휴대폰'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 222 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="od\_settle\_case" value="신용카드" id="od\_settle\_case06" <?php echo get\_checked($od\_settle\_case, '신용카드'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 224 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="od\_settle\_case" value="간편결제" id="od\_settle\_case07" <?php echo get\_checked($od\_settle\_case, '간편결제'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 226 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="od\_settle\_case" value="KAKAOPAY" id="od\_settle\_case08" <?php echo get\_checked($od\_settle\_case, 'KAKAOPAY'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 232 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="od\_misu" value="Y" id="od\_misu01" <?php echo get\_checked($od\_misu, 'Y'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 234 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="od\_cancel\_price" value="Y" id="od\_misu02" <?php echo get\_checked($od\_cancel\_price, 'Y'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="od\_refund\_price" value="Y" id="od\_misu03" <?php echo get\_checked($od\_refund\_price, 'Y'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 238 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="od\_receipt\_point" value="Y" id="od\_misu04" <?php echo get\_checked($od\_receipt\_point, 'Y'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 240 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="od\_coupon" value="Y" id="od\_misu05" <?php echo get\_checked($od\_coupon, 'Y'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 243 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="od\_escrow" value="Y" id="od\_misu06" <?php echo get\_checked($od\_escrow, 'Y'); ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 250 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" id="fr\_date" name="fr\_date" value="<?php echo $fr\_date; ?>" class="frm\_input" size="10" maxlength="10"> ~

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 251 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" id="to\_date" name="to\_date" value="<?php echo $to\_date; ?>" class="frm\_input" size="10" maxlength="10">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 264 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="search\_od\_status" value="<?php echo $od\_status; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 275 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col" id="th\_ordnum" rowspan="2" colspan="2"><a href="<?php echo title\_sort("od\_id", 1)."&amp;$qstr1"; ?>">주문번호</a></th>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 352 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

MD5 Hashing algorithm.

$uid = md5($row['od\_id'].$row['od\_time'].$row['od\_ip']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 364 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="orderlist<?php echo ' '.$bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 366 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_id[<?php echo $i ?>]" value="<?php echo $row['od\_id'] ?>" id="od\_id\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 367 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i; ?>" class="sound\_only">주문번호 <?php echo $row['od\_id']; ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 368 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk[]" value="<?php echo $i ?>" id="chk\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 371 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_SHOP\_URL; ?>/orderinquiryview.php?od\_id=<?php echo $row['od\_id']; ?>&amp;uid=<?php echo $uid; ?>" class="orderitem"><?php echo $disp\_od\_id; ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 372 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $od\_mobile; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 373 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $od\_paytype; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 375 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_odrer" class="td\_name"><?php echo $mb\_nick; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 376 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_odrertel" class="td\_tel"><?php echo get\_text($row['od\_tel']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 377 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_recvr" class="td\_name"><a href="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>?sort1=<?php echo $sort1; ?>&amp;sort2=<?php echo $sort2; ?>&amp;sel\_field=od\_b\_name&amp;search=<?php echo get\_text($row['od\_b\_name']); ?>"><?php echo get\_text($row['od\_b\_name']); ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 378 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td rowspan="3" class="td\_num td\_numsum"><?php echo number\_format($row['od\_cart\_price'] + $row['od\_send\_cost'] + $row['od\_send\_cost2']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 379 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td rowspan="3" class="td\_num\_right"><?php echo number\_format($row['od\_receipt\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 380 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td rowspan="3" class="td\_numcancel<?php echo $td\_color; ?> td\_num"><?php echo number\_format($row['od\_cancel\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 381 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td rowspan="3" class="td\_num\_right"><?php echo number\_format($row['couponprice']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 382 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td rowspan="3" class="td\_num\_right"><?php echo number\_format($row['od\_misu']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 384 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./orderform.php?od\_id=<?php echo $row['od\_id']; ?>&amp;<?php echo $qstr; ?>" class="mng\_mod btn btn\_02"><span class="sound\_only"><?php echo $row['od\_id']; ?> </span>보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 387 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 390 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>?sort1=<?php echo $sort1; ?>&amp;sort2=<?php echo $sort2; ?>&amp;sel\_field=mb\_id&amp;search=<?php echo $row['mb\_id']; ?>"><?php echo $row['mb\_id']; ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 395 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_odrcnt"><?php echo $row['od\_cart\_count']; ?>건</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 396 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_odrall"><?php echo $od\_cnt; ?>건</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 398 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 400 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="current\_status[<?php echo $i ?>]" value="<?php echo $row['od\_status'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 401 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $row['od\_status']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 404 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="current\_settle\_case[<?php echo $i ?>]" value="<?php echo $row['od\_settle\_case'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 405 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $s\_receipt\_way; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 409 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_invoice[<?php echo $i; ?>]" value="<?php echo $row['od\_invoice']; ?>" class="frm\_input" size="10">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 411 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo ($row['od\_invoice'] ? $row['od\_invoice'] : '-');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 416 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="od\_delivery\_company[<?php echo $i; ?>]">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 417 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_delivery\_company($delivery\_company); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 420 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo ($row['od\_delivery\_company'] ? $row['od\_delivery\_company'] : '-');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 425 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_invoice\_time[<?php echo $i; ?>]" value="<?php echo $invoice\_time; ?>" class="frm\_input" size="10" maxlength="19">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 427 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo (is\_null\_time($row['od\_invoice\_time']) ? '-' : substr($row['od\_invoice\_time'],2,14));

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 448 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($tot\_itemcount); ?>건</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 450 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($tot\_orderprice); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 451 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($tot\_receiptprice); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 452 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($tot\_ordercancel); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 453 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($tot\_couponprice); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 454 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($tot\_misu); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 473 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label><input type="checkbox" name="od\_status" value="<?php echo $change\_status; ?>"> '<?php echo $od\_status ?>'상태에서 '<strong><?php echo $change\_status ?></strong>'상태로 변경합니다.</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 476 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="od\_send\_mail"><?php echo $change\_status; ?>안내 메일</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 478 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="od\_send\_sms"><?php echo $change\_status; ?>안내 SMS</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 499 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 562 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.getElementById("fr\_date").value = "<?php echo date('Y-m-d', strtotime('-'.$date\_term.' days', G5\_SERVER\_TIME)); ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 568 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.getElementById("fr\_date").value = "<?php echo date('Y-m-d', strtotime('-'.$week\_term.' days', G5\_SERVER\_TIME)); ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 569 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.getElementById("to\_date").value = "<?php echo date('Y-m-d', strtotime('-'.($week\_term - 6).' days', G5\_SERVER\_TIME)); ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 571 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.getElementById("fr\_date").value = "<?php echo date('Y-m-01', strtotime('-1 Month', $last\_term)); ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 572 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.getElementById("to\_date").value = "<?php echo date('Y-m-t', strtotime('-1 Month', $last\_term)); ?>";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlistupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$receive\_number = preg\_replace("/[^0-9]/", "", $od['od\_hp']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlistupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace("/[^0-9]/", "", $default['de\_admin\_company\_tel']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlistupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$receive\_number = preg\_replace("/[^0-9]/", "", $od['od\_hp']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderlistupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace("/[^0-9]/", "", $default['de\_admin\_company\_tel']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderpartcancel.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_id" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderpartcancel.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $od['od\_settle\_case']; ?> 부분취소</h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderpartcancel.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 입력</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderpartcancel.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_price($od\_misu); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderpartcancel.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var max\_mny = parseInt(<?php echo $od\_misu; ?>);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderpartcancelupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$tax\_mny = isset($\_POST['mod\_tax\_mny']) ? preg\_replace('/[^0-9]/', '', $\_POST['mod\_tax\_mny']) : 0;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderpartcancelupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$free\_mny = isset($\_POST['mod\_free\_mny']) ? preg\_replace('/[^0-9]/', '', $\_POST['mod\_free\_mny']) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderpartcancelupdate.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

alert("<?php echo $od['od\_settle\_case']; ?> 부분취소 처리됐습니다.");

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 5 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr\_date = isset($\_REQUEST['fr\_date']) ? preg\_replace('/[^0-9 :\_\-]/i', '', $\_REQUEST['fr\_date']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to\_date = isset($\_REQUEST['to\_date']) ? preg\_replace('/[^0-9 :\_\-]/i', '', $\_REQUEST['to\_date']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr\_od\_id = isset($\_REQUEST['fr\_od\_id']) ? preg\_replace('/[^0-9]/i', '', $\_REQUEST['fr\_od\_id']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to\_od\_id = isset($\_REQUEST['to\_od\_id']) ? preg\_replace('/[^0-9]/i', '', $\_REQUEST['to\_od\_id']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$t = preg\_replace("/([0-9]{3})(.\*)([0-9]{4})/", "\\1-\\2-\\3", $t);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$t = preg\_replace("/([0-9]{2})(.\*)([0-9]{4})/", "\\1-\\2-\\3", $t);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$t = preg\_replace("/([0-9]{3})(.\*)([0-9]{4})/", "\\1-\\2-\\3", $t);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '"\''.$row['od\_b\_zip1'].$row['od\_b\_zip2'].'"\''.',';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '"'.$pull\_address.'"'.',';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '"'.$row['od\_b\_name'].'"'.',';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '"'.conv\_telno($row['od\_b\_tel']) . '"'.',';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '"'.conv\_telno($row['od\_b\_hp']) . '"'.',';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

echo '"'.preg\_replace("/\"/", "&#034;", $row['it\_name']) . '"'.',';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '"'.preg\_replace("/\"/", "&#034;", $row['it\_name']) . '"'.',';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '"'.$row['ct\_qty'].'"'.',';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '"'.$row['ct\_option'].'"'.',';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '"'.$ct\_send\_cost.'"'.',';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '"\''.$row['it\_id'].'\'"'.',';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '"\''.$row['od\_id'].'\'"'.',';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '"'.$row['od\_invoice'].'"'.',';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

echo '"'.preg\_replace("/\"/", "&#034;", $row['od\_memo']).'"';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '"'.preg\_replace("/\"/", "&#034;", $row['od\_memo']).'"';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 225 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

preg\_replace("/\"/", "&#034;", $row['it\_name']),

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 232 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

preg\_replace("/\"/", "&#034;", $row['od\_memo']));

**STANDARD: Potentially Unsafe Code - fopen**

Line: 332 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

$fh=fopen($fname, "rb");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 332 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fh=fopen($fname, "rb");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 382 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $fr\_date.' 부터 '.$to\_date.' 까지 '.$ct\_status.' 내역';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 384 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $fr\_od\_id.' 부터 '.$to\_od\_id.' 까지 '.$ct\_status.' 내역';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 418 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2>주문번호 <?php echo $row1['od\_id']; ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 419 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h3>보내는 사람 : <?php echo get\_text($row1['od\_name']); ?></h3>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 423 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo get\_text($row1['od\_addr']); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 425 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo get\_text($row1['od\_hp']); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 427 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo get\_text($row1['od\_tel']); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 432 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h3>받는 사람 : <?php echo get\_text($row1['od\_b\_name']); ?></h3>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 435 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo get\_text($row1['od\_b\_addr']); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 437 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo get\_text($row1['od\_b\_hp']); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 439 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo get\_text($row1['od\_b\_tel']); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 530 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $it\_name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 531 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($it\_price); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 532 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_cntsmall"><?php echo $fontqty1; ?><?php echo number\_format($row2['ct\_qty']); ?><?php echo $fontqty2; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 533 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num td\_numsum"><?php echo number\_format($row2\_tot\_price); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 534 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_sendcost\_by"><?php echo $ct\_send\_cost; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 542 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($row1['od\_send\_cost']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 543 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_cntsmall"><?php echo $fontqty1; ?>1<?php echo $fontqty2; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 544 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num td\_numsum"><?php echo number\_format($row1['od\_send\_cost']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 549 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($row1['od\_send\_cost2']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 550 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_cntsmall"><?php echo $fontqty1; ?>1<?php echo $fontqty2; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 551 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num td\_numsum"><?php echo number\_format($row1['od\_send\_cost2']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 558 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($sub\_tot\_qty + 2); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 559 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($sub\_tot\_price + $row1['od\_send\_cost'] + $row1['od\_send\_cost2']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 584 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($tot\_tot\_qty); ?></strong>개

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 585 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\orderprintresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($tot\_tot\_price); ?></strong>원

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 5 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\ordersms.inc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$receive\_number = preg\_replace("/[^0-9]/", "", $od\_hp);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\ordersms.inc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace("/[^0-9]/", "", $default['de\_admin\_company\_tel']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaycopy.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="pp\_id" value="<?php echo $pp\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaycopy.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaycopy.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="pp\_name" value="<?php echo $row['pp\_name']; ?>" id="pp\_name" required class="required frm\_input"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaycopy.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="od\_id" value="<?php echo $row['od\_id']; ?>" id="od\_id" class="frm\_input"></td>

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_personalpay\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_personalpay\_table']}`

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="pp\_id" value="<?php echo $pp\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="popup" value="<?php echo $popup; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $wrp\_tag\_st; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($popup != 'yes') echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="pp\_name" value="<?php echo get\_text($pp['pp\_name']); ?>" id="pp\_name" required class="required frm\_input"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="pp\_price" value="<?php echo $pp['pp\_price']; ?>" id="pp\_price" required class="required frm\_input" size="15"> 원</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="od\_id" value="<?php echo $pp['od\_id'] ? $pp['od\_id'] : ''; ?>" id="od\_id" class="frm\_input" size="20"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><textarea name="pp\_content" id="pp\_content" rows="8"><?php echo html\_purifier($pp['pp\_content']); ?></textarea></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="pp\_receipt\_price" value="<?php echo $pp['pp\_receipt\_price'] ? $pp['pp\_receipt\_price'] : ''; ?>" id="pp\_receipt\_price" class="frm\_input" size="15"> 원</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="" <?php echo get\_selected($pp['pp\_settle\_case'], ''); ?>>선택</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="무통장" <?php echo get\_selected($pp['pp\_settle\_case'], '무통장'); ?>>무통장</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="계좌이체" <?php echo get\_selected($pp['pp\_settle\_case'], '계좌이체'); ?>>계좌이체</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="가상계좌" <?php echo get\_selected($pp['pp\_settle\_case'], '가상계좌'); ?>>가상계좌</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="신용카드" <?php echo get\_selected($pp['pp\_settle\_case'], '신용카드'); ?>>신용카드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 160 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="휴대폰" <?php echo get\_selected($pp['pp\_settle\_case'], '휴대폰'); ?>>휴대폰</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 169 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="pp\_receipt\_time" value="<?php echo is\_null\_time($pp['pp\_receipt\_time']) ? "" : $pp['pp\_receipt\_time']; ?>" id="pp\_receipt\_time" class="frm\_input" maxlength="19">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 217 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $cash\_receipt\_script; ?>">현금영수증 확인</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 219 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="window.open('<?php echo G5\_SHOP\_URL; ?>/taxsave.php?tx=personalpay&od\_id=<?php echo $pp\_id; ?>', 'taxsave', 'width=550,height=400,scrollbars=1,menus=0');">현금영수증 발급</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 230 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><textarea name="pp\_shop\_memo" id="pp\_shop\_memo" rows="8"><?php echo $pp['pp\_shop\_memo']; ?></textarea></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1" <?php echo get\_selected($pp['pp\_use'], 1); ?>>사용함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 237 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo get\_selected($pp['pp\_use'], 0); ?>>사용안함</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 250 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="<?php echo $btn\_class; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 255 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./personalpaylist.php?<?php echo $qstr; ?>" class="btn btn\_02">목록</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 258 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./personalpayformupdate.php?w=d&amp;pp\_id=<?php echo $pp['pp\_id']; ?>" onclick="return delete\_confirm(this);" class="btn btn\_02">삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 262 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $wrp\_tag\_end; ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$pp\_id = isset($\_REQUEST['pp\_id']) ? preg\_replace('/[^0-9]/', '', $\_REQUEST['pp\_id']) : 0;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpayformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$pp\_price = isset($\_POST['pp\_price']) ? preg\_replace('/[^0-9]/', '', $\_REQUEST['pp\_price']) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">전체 </span><span class="ov\_num"> <?php echo number\_format($total\_count) ?>건 </span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="pp\_id"<?php echo get\_selected($sfl, "pp\_id"); ?>>개인결제번호</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="pp\_name"<?php echo get\_selected($sfl, "pp\_name"); ?>>이름</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="od\_id"<?php echo get\_selected($sfl, "od\_id"); ?>>주문번호</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx ?>" id="stx" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="pp\_id\_<?php echo $i; ?>" name="pp\_id[<?php echo $i; ?>]" value="<?php echo $row['pp\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="chk\_<?php echo $i; ?>" name="chk[]" value="<?php echo $i; ?>" title="내역선택">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><?php echo get\_text($row['pp\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_odrnum3"><?php echo $od\_id; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numsum"><?php echo number\_format($row['pp\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($row['pp\_receipt\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numrdy"><?php echo number\_format($row['pp\_price'] - $row['pp\_receipt\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_payby"><?php echo $row['pp\_settle\_case']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_date"><?php echo is\_null\_time($row['pp\_receipt\_time']) ? '' : substr($row['pp\_receipt\_time'], 2, 8); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_boolean"><?php echo $row['pp\_use'] ? '예' : '아니오'; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./personalpayform.php?w=u&amp;pp\_id=<?php echo $row['pp\_id']; ?>&amp;<?php echo $qstr; ?>" class="btn btn\_03"><span class="sound\_only"><?php echo $row['pp\_id']; ?> </span>수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./personalpaycopy.php?pp\_id=<?php echo $row['pp\_id']; ?>" class="personalpaycopy btn btn\_02"><span class="sound\_only"><?php echo $row['pp\_id']; ?> </span>복사</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">자료가 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\personalpaylistdelete.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ppp\_id = isset($\_POST['pp\_id'][$i]) ? preg\_replace('/[^0-9]/', '', $\_POST['pp\_id'][$k]) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\price.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\price.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $pg\_anchor; ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr\_date = isset($\_REQUEST['fr\_date']) ? preg\_replace('/[^0-9 :\_\-]/i', '', $\_REQUEST['fr\_date']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to\_date = isset($\_REQUEST['to\_date']) ? preg\_replace('/[^0-9 :\_\-]/i', '', $\_REQUEST['to\_date']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr\_date = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3", $fr\_date);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to\_date = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3", $to\_date);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$date = preg\_replace("/-/", "", $save['od\_date']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_alignc"><a href="./sale1today.php?date=<?php echo $date; ?>"><?php echo $save['od\_date']; ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($save['ordercount']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numsum"><?php echo number\_format($save['orderprice']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numcoupon"><?php echo number\_format($save['ordercoupon']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receiptbank']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receiptvbank']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receiptiche']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receiptcard']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receipteasy']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receipthp']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receiptpoint']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numcancel1"><?php echo number\_format($save['ordercancel']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numrdy"><?php echo number\_format($save['misu']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['ordercount']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['orderprice']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['ordercoupon']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receiptbank']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receiptvbank']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receiptiche']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receiptcard']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receipteasy']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receipthp']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receiptpoint']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['ordercancel']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1date.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['misu']); ?></td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr\_month = isset($\_REQUEST['fr\_month']) ? preg\_replace('/[^0-9 :\_\-]/i', '', $\_REQUEST['fr\_month']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to\_month = isset($\_REQUEST['to\_month']) ? preg\_replace('/[^0-9 :\_\-]/i', '', $\_REQUEST['to\_month']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr\_month = preg\_replace("/([0-9]{4})([0-9]{2})/", "\\1-\\2", $fr\_month);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to\_month = preg\_replace("/([0-9]{4})([0-9]{2})/", "\\1-\\2", $to\_month);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$date = preg\_replace("/-/", "", $save['od\_date']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_alignc"><a href="./sale1date.php?fr\_date=<?php echo $date; ?>01&amp;to\_date=<?php echo $date; ?>31"><?php echo $save['od\_date']; ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($save['ordercount']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numsum"><?php echo number\_format($save['orderprice']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numcoupon"><?php echo number\_format($save['ordercoupon']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receiptbank']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receiptvbank']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receiptiche']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receiptcard']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receipteasy']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receipthp']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receiptpoint']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numcancel1"><?php echo number\_format($save['ordercancel']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numrdy"><?php echo number\_format($save['misu']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['ordercount']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['orderprice']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['ordercoupon']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receiptbank']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receiptvbank']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receiptiche']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receiptcard']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receipteasy']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receipthp']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receiptpoint']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['ordercancel']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1month.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['misu']); ?></td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$date = isset($\_GET['date']) ? preg\_replace('/[^0-9]/i', '', $\_GET['date']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$date = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3", $date);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_alignc"><a href="./orderform.php?od\_id=<?php echo $row['od\_id']; ?>"><?php echo $row['od\_id']; ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_name"><?php echo $href; ?><?php echo $row['od\_name']; ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numsum"><?php echo number\_format($row['orderprice']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($row['couponprice']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($receipt\_bank); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($receipt\_vbank); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($receipt\_iche); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($receipt\_card); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($receipt\_easy); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($receipt\_hp); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($row['od\_receipt\_point']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numcancel1"><?php echo number\_format($row['od\_cancel\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numrdy"><?php echo number\_format($row['od\_misu']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['orderprice']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['coupon']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receipt\_bank']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receipt\_vbank']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receipt\_iche']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receipt\_card']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receipt\_easy']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receipt\_hp']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receipt\_point']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['ordercancel']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1today.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['misu']); ?></td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr\_year = isset($\_REQUEST['fr\_year']) ? preg\_replace('/[^0-9 :\_\-]/i', '', $\_REQUEST['fr\_year']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to\_year = isset($\_REQUEST['to\_year']) ? preg\_replace('/[^0-9 :\_\-]/i', '', $\_REQUEST['to\_year']) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_alignc"><a href="./sale1month.php?fr\_month=<?php echo $save['od\_date']; ?>01&amp;to\_month=<?php echo $save['od\_date']; ?>12"><?php echo $save['od\_date']; ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($save['ordercount']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numsum"><?php echo number\_format($save['orderprice']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numcoupon"><?php echo number\_format($save['ordercoupon']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receiptbank']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receiptvbank']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receiptiche']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receiptcard']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receipteasy']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receipthp']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numincome"><?php echo number\_format($save['receiptpoint']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numcancel1"><?php echo number\_format($save['ordercancel']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numrdy"><?php echo number\_format($save['misu']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['ordercount']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['orderprice']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['ordercoupon']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receiptbank']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receiptvbank']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receiptiche']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receiptcard']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receipteasy']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receipthp']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['receiptpoint']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['ordercancel']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sale1year.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num\_right"><?php echo number\_format($tot['misu']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sendcostlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sendcostlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sendcostlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="sc\_id\_<?php echo $i; ?>" name="sc\_id[<?php echo $i; ?>]" value="<?php echo $row['sc\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sendcostlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="chk\_<?php echo $i; ?>" name="chk[]" value="<?php echo $i; ?>" title="내역선택">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sendcostlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><?php echo $row['sc\_name']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sendcostlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_postalbig"><?php echo $row['sc\_zip1'].' ~ '.$row['sc\_zip2']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sendcostlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_sendcost\_add"><?php echo number\_format($row['sc\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sendcostlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sendcostupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sc\_zip1 = isset($\_POST['sc\_zip1']) ? preg\_replace('/[^0-9]/', '', $\_POST['sc\_zip1']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sendcostupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sc\_zip2 = isset($\_POST['sc\_zip2']) ? preg\_replace('/[^0-9]/', '', $\_POST['sc\_zip2']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\sendcostupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sc\_price = isset($\_POST['sc\_price']) ? preg\_replace('/[^0-9]/', '', $\_POST['sc\_price']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\wishlist.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fr = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3", $fr\_date);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\wishlist.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$to = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3", $to\_date);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $listall; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">전체 </span><span class="ov\_num"> <?php echo $total\_count; ?>건</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="doc" value="<?php echo $doc; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<option value='{$row1['ca\_id']}'".get\_selected($row1['ca\_id'], $sel\_ca\_id).">$nbsp{$row1['ca\_name']}\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="fr\_date" value="<?php echo $fr\_date; ?>" id="fr\_date" required class="required frm\_input" size="8" maxlength="8">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="to\_date" value="<?php echo $to\_date; ?>" id="to\_date" required class="required frm\_input" size="8" maxlength="8">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $num; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $href; ?>"><?php echo get\_it\_image($row['it\_id'], 50, 50); ?> <?php echo cut\_str($row['it\_name'],30); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $row['it\_id\_cnt']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\shop\_admin\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr1&amp;page="); ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_form.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fg\_no = isset($\_REQUEST['fg\_no']) ? preg\_replace('/[^0-9]/i', '', $\_REQUEST['fg\_no']) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><a href="javascript:sms\_obj.person(1)"><?php echo $no\_group['bg\_name']?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($no\_group['bg\_receipt'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mngsmall"><button type="button" class="btn\_frmline" onclick="sms\_obj.group\_add(1, '<?php echo $no\_group['bg\_name']?>', '<?php echo number\_format($no\_group['bg\_receipt'])?>')">추가</button></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><a href="javascript:sms\_obj.person(<?php echo $group[$i]['bg\_no']?>)"><?php echo $group[$i]['bg\_name']?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($group[$i]['bg\_receipt'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mngsmall"><button type="button" class="btn\_frmline" onclick="sms\_obj.group\_add(<?php echo $group[$i]['bg\_no']?>, '<?php echo $group[$i]['bg\_name']?>', '<?php echo number\_format($group[$i]['bg\_receipt'])?>')">추가</button></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="<?php echo $colspan?>" class="td\_mbstat">데이터가 없습니다.</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bk\_no\_<?php echo $res['bk\_no']; ?>" class="sound\_only"><?php echo get\_text($res['bk\_name']) ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bk\_no" value="<?php echo $res['bk\_no']?>" id="bk\_no\_<?php echo $res['bk\_no']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <td class="td\_name"><?php echo $group\_name?></td> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbname"><?php echo get\_text($res['bk\_name']) ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $res['bk\_hp']?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <td class="td\_boolean"><?php echo $res['bk\_receipt'] ? '수신' : '거부'?></td> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <td class="td\_boolean"><?php echo $res['bk\_receipt'] ? '예' : ''?></td> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_boolean"><?php echo $res['mb\_id'] ? '회원' : '비회원'?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mngsmall"><button type="button" class="btn\_frmline" onclick="sms\_obj.person\_add(<?php echo $res['bk\_no']?>, '<?php echo get\_text($res['bk\_name']) ?>', '<?php echo $res['bk\_hp']?>')">추가</button></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="search\_form" id="sms\_person\_form" method="get" action="<?php echo $\_SERVER['SCRIPT\_NAME']?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="total\_pg" value="<?php echo $total\_page?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value=""<?php echo get\_selected('', $bg\_no); ?>> 전체 </option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"<?php echo get\_selected(1, $bg\_no); ?>> <?php echo $no\_group['bg\_name']?> (<?php echo number\_format($no\_group['bg\_receipt'])?> 명) </option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $group[$i]['bg\_no']?>" <?php echo get\_selected($bg\_no, $group[$i]['bg\_no']); ?>> <?php echo $group[$i]['bg\_name']?> (<?php echo number\_format($group[$i]['bg\_receipt'])?> 명) </option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="all"<?php echo get\_selected('all', $st); ?>>이름 + 번호</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="name"<?php echo get\_selected('name', $st); ?>>이름</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="hp"<?php echo get\_selected('hp', $st); ?>>번호</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" size="15" name="sv" value="<?php echo $sv?>" id="svv" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

총 건수 : <?php echo number\_format($total\_count)?> /

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

회원 : <?php echo number\_format($member\_count)?> /

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

비회원 : <?php echo number\_format($no\_member\_count)?> /

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

수신 : <?php echo number\_format($receipt\_count)?> /

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\ajax.sms\_write\_person.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

거부 : <?php echo number\_format($reject\_count)?>

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\config.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = "ALTER TABLE `{$g5['config\_table']}`

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cf\_icode\_server\_ip" value="<?php echo $config['cf\_icode\_server\_ip']?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cf\_sms\_use" value="<?php echo $config['cf\_sms\_use']?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="" <?php echo get\_selected($config['cf\_sms\_type'], ''); ?>>SMS</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="LMS" <?php echo get\_selected($config['cf\_sms\_type'], 'LMS'); ?>>LMS</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_icode\_id" value="<?php echo $config['cf\_icode\_id']; ?>" id="cf\_icode\_id" class="frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="password" name="cf\_icode\_pw" value="<?php echo $config['cf\_icode\_pw']; ?>" id="cf\_icode\_pw" class="frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="icode\_old\_version <?php if(!(isset($userinfo['payment']) && $userinfo['payment'])){ echo 'cf\_tr\_hide'; } ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo number\_format($userinfo['coin'])?> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="http://www.icodekorea.com/smsbiz/credit\_card\_amt.php?icode\_id=<?php echo $config['cf\_icode\_id']; ?>&amp;icode\_passwd=<?php echo $config['cf\_icode\_pw']; ?>" target="\_blank" class="btn\_frmline">충전하기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="cf\_icode\_token\_key" value="<?php echo $config['cf\_icode\_token\_key']; ?>" id="cf\_icode\_token\_key" class="frm\_input" size="40">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

서버아이피 : <?php echo $\_SERVER['SERVER\_ADDR']; ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\config\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$cf\_icode\_server\_port = isset($cf\_icode\_server\_port) ? preg\_replace('/[^0-9]/', '', $cf\_icode\_server\_port) : '7295';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\emoticon\_move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\emoticon\_move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sw" value="<?php echo $sw ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\emoticon\_move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fo\_no\_list" value="<?php echo $fo\_no\_list ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\emoticon\_move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" value="<?php echo $list[$i]['fg\_no'] ?>" id="chk<?php echo $i ?>" name="chk\_fg\_no[]">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\emoticon\_move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk<?php echo $i ?>"><?php echo $list[$i]['fg\_name'] ?></label>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\emoticon\_move\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fo\_no\_list = isset($\_POST['fo\_no\_list']) ? preg\_replace('/[^a-zA-Z0-9\, ]/', '', $\_POST['fo\_no\_list']) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\emoticon\_move\_update.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

alert("<?php echo $msg; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\emoticon\_move\_update.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

opener.document.location.href = "<?php echo $opener\_href; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\emoticon\_move\_update.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $msg; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\emoticon\_move\_update.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $opener\_href; ?>">돌아가기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="group<?php echo isset($res['fg\_no']) ? $res['fg\_no'] : ''; ?>" method="post" action="./form\_group\_update.php" class="local\_sch03 local\_sch">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fg\_no" value="<?php echo isset($res['fg\_no']) ? $res['fg\_no'] : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="count\_add01">건수 : <?php echo $total\_count ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="group<?php echo isset($group[$i]['fg\_no']) ? $group[$i]['fg\_no'] : ''; ?>" method="post" action="./form\_group\_update.php" onsubmit="return grouplist\_submit(this);">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($res['cnt'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $group[$i]['fg\_no']?>"> <?php echo $group[$i]['fg\_name']?> </option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fg\_no[<?php echo $i ?>]" value="<?php echo $group[$i]['fg\_no']?>" id="fg\_no\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i ?>" class="sound\_only"><?php echo $group[$i]['fg\_name']?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk[]" value="<?php echo $i ?>" id="chk\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="fg\_name\_<?php echo $i; ?>" class="sound\_only">그룹명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="fg\_member[<?php echo $i; ?>]" value="1" id="fg\_member\_<?php echo $i; ?>" <?php if ($group[$i]['fg\_member']) echo 'checked';?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="fg\_member\_<?php echo $i; ?>">회원</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo number\_format($group[$i]['fg\_count'])?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="select\_fg\_no\_<?php echo $i; ?>" class="sound\_only">그룹명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="select\_fg\_no[<?php echo $i; ?>]" id="select\_fg\_no\_<?php echo $i; ?>" onchange="move(<?php echo $group[$i]['fg\_no']?>, '<?php echo $group[$i]['fg\_name']?>', this);">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $group[$j]['fg\_no']?>"> <?php echo $group[$j]['fg\_name']?></option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./form\_list.php?fg\_no=<?php echo $group[$i]['fg\_no']?>" class="btn btn\_03">보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

location.href = "./form\_update.php?w=d&fo\_no=" + fo\_no + "&page=<?php echo $page?>&fg\_no=<?php echo $fg\_no?>&st=<?php echo get\_text($st); ?>&sv=<?php echo get\_text($sv); ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">건수</span><span class="ov\_num"><?php echo number\_format($total\_count);?>건</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="fg\_no" id="fg\_no" onchange="location.href='<?php echo $\_SERVER['SCRIPT\_NAME']?>?fg\_no='+this.value;">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="" <?php echo $fg\_no?'':'selected'?>> 전체 </option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0" <?php echo $fg\_no=='0'?'selected':''?>> 미분류 (<?php echo number\_format($no\_count)?>) </option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $group[$i]['fg\_no']?>" <?php echo ($fg\_no==$group[$i]['fg\_no'])?'selected':''?>> <?php echo $group[$i]['fg\_name']?> (<?php echo number\_format($group[$i]['fg\_count'])?>) </option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="search\_form" method="get" action="<?php echo $\_SERVER['SCRIPT\_NAME']?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fg\_no" value="<?php echo $fg\_no;?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="all"<?php echo get\_selected('all', $st); ?>>제목 + 이모티콘</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="name"<?php echo get\_selected('name', $st); ?>>제목</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="content"<?php echo get\_selected('content', $st); ?>>이모티콘</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="sv" value="<?php echo get\_text($sv) ;?>" id="sv" required class="frm\_input required" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo $token; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fg\_no" value="<?php echo $fg\_no; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="li\_<?php echo $li\_i; ?> sms5\_box">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="fo\_no\_<?php echo $i; ?>" class="sound\_only"><?php echo $group\_name?>의 <?php echo cut\_str($res['fo\_name'],10)?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 174 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="fo\_no[]" value="<?php echo $res['fo\_no']?>" id="fo\_no\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea readonly class="box\_txt box\_square"><?php echo $res['fo\_content']?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">그룹 </span><b><?php echo $group\_name?></b><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 181 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">제목 </span><?php echo cut\_str($res['fo\_name'],10)?><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 184 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">등록 </span><?php echo date('Y-m-d', strtotime($res['fo\_datetime']))?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./form\_write.php?w=u&amp;fo\_no=<?php echo $res['fo\_no']?>&amp;page=<?php echo $page;?>&amp;fg\_no=<?php echo $fg\_no;?>&amp;st=<?php echo get\_text($st);?>&amp;sv=<?php echo get\_text($sv);?>">수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:void(book\_del('<?php echo $res['fo\_no']?>'));">삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 189 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./sms\_write.php?fo\_no=<?php echo $res['fo\_no']?>">보내기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 198 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./form\_write.php?page=<?php echo $page?>&amp;fg\_no=<?php echo $fg\_no?>" class="btn btn\_01">이모티콘 추가</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 239 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, $\_SERVER['SCRIPT\_NAME']."?fg\_no=$fg\_no&amp;st=$st&amp;sv=$sv&amp;page=");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fo\_no" value="<?php echo $write['fo\_no']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="get\_fg\_no" value="<?php echo $fg\_no?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title'];?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $res['fg\_no']?>"<?php echo get\_selected($res['fg\_no'], $write['fg\_no']); ?>><?php echo $res['fg\_name']?></option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="fo\_content" id="sms\_contents" class="box\_txt box\_square" onkeyup="byte\_check('sms\_contents', 'sms\_bytes');" accesskey="m"><?php echo $write['fo\_content']?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td> <?php echo $write['fo\_datetime']?> </td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\form\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./form\_list.php?<?php echo clean\_query\_string($\_SERVER['QUERY\_STRING']); ?>">목록</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="search\_form" id="search\_form" action=<?php echo $\_SERVER['SCRIPT\_NAME'];?> class="local\_sch01 local\_sch" method="get">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="sv" value="<?php echo $sv ?>" id="sv" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="<?php echo $colspan?>" class="empty\_table" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numsmall"><?php echo $vnum--?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><span title="<?php echo $res['wr\_message']?>"><?php echo $res['wr\_message']?></span></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_tel"><?php echo $res['wr\_reply']?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo date('Y-m-d H:i', strtotime($res['wr\_datetime']))?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_boolean"><?php echo $res['wr\_booking']!='0000-00-00 00:00:00'?"<span title='{$res['wr\_booking']}'>예약</span>":'';?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($res['wr\_total'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($res['wr\_success'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($res['wr\_failure'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $dupli\_count;?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($res['wr\_re\_total'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./history\_view.php?page=<?php echo $page;?>&amp;st=<?php echo $st;?>&amp;sv=<?php echo $sv;?>&amp;wr\_no=<?php echo $res['wr\_no'];?>" class="btn btn\_03">수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <a href="./history\_del.php?page=<?php echo $page;?>&amp;st=<?php echo $st;?>&amp;sv=<?php echo $sv;?>&amp;wr\_no=<?php echo $res['wr\_no'];?>">삭제</a> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, $\_SERVER['SCRIPT\_NAME']."?st=$st&amp;sv=$sv&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="search\_form" method="get" action="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>" class="local\_sch01 local\_sch" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="hs\_name"<?php echo get\_selected('hs\_name', $st); ?>>이름</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="hs\_hp"<?php echo get\_selected('hs\_hp', $st); ?>>휴대폰번호</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="bk\_no"<?php echo get\_selected('bk\_no', $st); ?>>고유번호</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="sv" value="<?php echo $sv; ?>" id="sv" required class="required frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="<?php echo $colspan; ?>" class="empty\_table" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $vnum--; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbname"><?php echo $bg\_name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbname"><a href="./num\_book\_write.php?w=u&amp;bk\_no=<?php echo $res['bk\_no']; ?>"><?php echo $res['hs\_name']; ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbid"><?php echo $mb\_id; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig"><?php echo $res['hs\_hp']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo date('Y-m-d H:i', strtotime($write['wr\_datetime']))?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_boolean"><?php echo $write['wr\_booking']!='0000-00-00 00:00:00'?"<span title='{$write['wr\_booking']}'>예약</span>":'';?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_boolean"><?php echo $res['hs\_flag']?'성공':'실패'?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_left"><span title="<?php echo $write['wr\_message']?>"><?php echo $write['wr\_message']?></span></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./history\_view.php?page=<?php echo $page; ?>&amp;st=<?php echo $st; ?>&amp;sv=<?php echo $sv; ?>&amp;wr\_no=<?php echo $res['wr\_no']; ?>" class="btn btn\_03">수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_num.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, $\_SERVER['SCRIPT\_NAME']."?st=$st&amp;sv=$sv&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 231 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_send.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

location.href = 'history\_view.php?wr\_no=<?php echo $wr\_no?>&wr\_renum=<?php echo $new\_wr\_renum?>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

location.href = './history\_send.php?w=f&page=<?php echo $page?>&st=<?php echo $st?>&sv=<?php echo $sv?>&wr\_no=<?php echo $wr\_no?>&wr\_renum=<?php echo $wr\_renum?>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

location.href = './sms\_write.php?wr\_no=<?php echo $wr\_no?>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="search\_form" method="get" action="<?php echo $\_SERVER['SCRIPT\_NAME']?>" class="local\_sch01 local\_sch">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="hs\_name" <?php echo get\_selected('hs\_name', $sst); ?>>이름</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="hs\_hp" <?php echo get\_selected('hs\_hp', $sst); ?>>휴대폰번호</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">전송건수</span><span class="ov\_num"> <?php echo number\_format($write['wr\_total'])?> 건</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">성공건수 </span><span class="ov\_num"><?php echo number\_format($write['wr\_success'])?> 건</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">실패건수 </span><span class="ov\_num"><?php echo number\_format($write['wr\_failure'])?> 건</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">전송일시 </span><span class="ov\_num"><?php echo $write['wr\_datetime']?></span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">예약일시 </span><span class="ov\_num"><?php echo $write['wr\_booking']?></span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">회신번호 </span><span class="ov\_num"><?php echo $write['wr\_reply']?></span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea class="box\_txt is\_overview" readonly><?php echo $write['wr\_message'];?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $re\_vnum--?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <td><?php echo $res['wr\_message']; ?></span></td>-->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <td><?php echo $res['wr\_reply']; ?></td>-->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $res['wr\_datetime']?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($res['wr\_total'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($res['wr\_success'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($res['wr\_failure'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./history\_view.php?page=<?php echo $page?>&amp;st=<?php echo $st?>&amp;sv=<?php echo $sv?>&amp;wr\_no=<?php echo $res['wr\_no']?>&amp;wr\_renum=<?php echo $res['wr\_renum']?>" class="btn btn\_03">수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <a href="./history\_del.php?page=<?php echo $page?>&amp;st=<?php echo $st?>&amp;sv=<?php echo $sv?>&amp;wr\_no=<?php echo $res['wr\_no']?>&amp;wr\_renum=<?php echo $res['wr\_renum']?>">삭제</a> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2>중복번호 <?php echo $tmp\_wr\_memo['total'];?>건</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><b><?php echo $key;?></b> 중복 <?php echo $v;?>건</li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 185 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2>문자전송 목록 <?php echo $re\_text?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 191 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./history\_list.php?page=<?php echo $page?>&amp;st=<?php echo $st?>&amp;sv=<?php echo $sv?>">목록</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 193 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./history\_view.php?page=<?php echo $page?>&amp;st=<?php echo $st?>&amp;sv=<?php echo $sv?>&amp;wr\_no=<?php echo $wr\_no?>">뒤로가기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 215 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="<?php echo $colspan?>" class="empty\_table">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 238 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 239 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numsmall"><?php echo number\_format($vnum--)?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 240 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_name"><?php echo $bg\_name?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 241 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbname"><?php echo $res['hs\_name']?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 242 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbid"><?php echo $mb\_id?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 243 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig"><?php echo $res['hs\_hp']?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 244 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo $res['hs\_datetime']?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 245 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_boolean"><?php echo $res['hs\_flag']?'성공':'실패'?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 247 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<u>결과코드</u> : <?php echo $res['hs\_code']?><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 248 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<u>로그</u> : <?php echo $res['hs\_log']?><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 249 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<u>메모</u> : <?php echo $res['hs\_memo']?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 253 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./history\_num.php?wr\_id=<?php echo $res['wr\_no']?>&amp;st=bk\_no&amp;sv=<?php echo $res['bk\_no']?>" class="btn\_03 btn">내역</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 255 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./history\_num.php?wr\_id=<?php echo $res['wr\_no']?>&amp;st=hs\_hp&amp;sv=<?php echo $res['hs\_hp']?>" class="btn\_03 btn">내역</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 265 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\history\_view.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo sms5\_sub\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $spage, $total\_spage, $\_SERVER['SCRIPT\_NAME']."?wr\_no=$wr\_no&amp;wr\_renum=$wr\_renum&amp;page=$page&amp;st=$st&amp;sv=$sv&amp;sst=$sst&amp;ssv=$ssv", "", "spage"); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\install.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="hidden\_form" method="post" action="<?php echo $\_SERVER['SCRIPT\_NAME']?>">

**STANDARD: Potentially Unsafe Code - eval**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\install.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

eval("\$file = \"$file\";");

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\install.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

eval("\$file = \"$file\";");

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\number\_move\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$bk\_no\_list = isset($\_POST['bk\_no\_list']) ? preg\_replace('/[^a-zA-Z0-9\, ]/', '', $\_POST['bk\_no\_list']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$bg\_no = isset($\_REQUEST['bg\_no']) ? preg\_replace('/[^0-9]/i', '', $\_REQUEST['bg\_no']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$st = isset($\_REQUEST['st']) ? preg\_replace('/[^a-z0-9]/i', '', $\_REQUEST['st']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$no\_hp = isset($\_GET['no\_hp']) ? preg\_replace('/[^0-9a-z\_]/i', '', $\_GET['no\_hp']) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var url = './num\_book.php?bg\_no=<?php echo $bg\_no?>&st=<?php echo $st?>&sv=<?php echo $sv?>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">업데이트 </span><span class="ov\_num"><?php echo isset($sms5['cf\_datetime']) ? $sms5['cf\_datetime'] : ''; ?></span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt"> 건수 </span><span class="ov\_num"><?php echo number\_format($total\_count)?>명</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt"> 회원 </span><span class="ov\_num"> <?php echo number\_format($member\_count)?>명</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt"> 비회원 </span><span class="ov\_num"> <?php echo number\_format($no\_member\_count)?>명</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt"> 수신 </span><span class="ov\_num"> <?php echo number\_format($receipt\_count)?>명</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt"> 거부 </span><span class="ov\_num"> <?php echo number\_format($reject\_count)?>명</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="search\_form" method="get" action="<?php echo $\_SERVER['SCRIPT\_NAME']?>" class="local\_sch01 local\_sch">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bg\_no" value="<?php echo $bg\_no?>" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="all"<?php echo get\_selected('all', $st); ?>>이름 + 휴대폰번호</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="name"<?php echo get\_selected('name', $st); ?>>이름</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="hp" <?php echo get\_selected('hp', $st); ?>>휴대폰번호</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="sv" value="<?php echo $sv?>" id="sv" required class="frm\_input required">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="bg\_no" id="bg\_no" onchange="location.href='<?php echo $\_SERVER['SCRIPT\_NAME']?>?bg\_no='+this.value;">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value=""<?php echo get\_selected('', $bg\_no); ?>> 전체 </option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $no\_group['bg\_no']?>"<?php echo get\_selected($no\_group['bg\_no'], $bg\_no); ?>> <?php echo $no\_group['bg\_name']?> (<?php echo number\_format($no\_group['bg\_count'])?> 명) </option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $group[$i]['bg\_no']?>"<?php echo get\_selected($group[$i]['bg\_no'], $bg\_no);?>> <?php echo $group[$i]['bg\_name']?> (<?php echo number\_format($group[$i]['bg\_count'])?> 명) </option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="no\_hp" id="no\_hp" <?php echo $no\_hp\_checked?> onclick="no\_hp\_click(this.checked)">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo $token; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="str\_query" value="<?php echo clean\_query\_string($\_SERVER['QUERY\_STRING']); ?>" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 175 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="<?php echo $colspan?>" class="empty\_table">데이터가 없습니다.</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 189 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 191 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bk\_no\_<?php echo $i; ?>" class="sound\_only"><?php echo $group\_name?>의 <?php echo get\_text($res['bk\_name']) ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 192 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="bk\_no[]" value="<?php echo $res['bk\_no']?>" id="bk\_no\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 194 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($vnum--)?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $group\_name?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 196 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbname"><?php echo get\_text($res['bk\_name']) ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 197 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig"><?php echo $res['bk\_hp']?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 198 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_boolean"><?php echo $res['bk\_receipt'] ? '<font color=blue>수신</font>' : '<font color=red>거부</font>'?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 199 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_mbid"><?php echo $res['mb\_id'] ? $res['mb\_id'] : '비회원'?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 200 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo $res['bk\_datetime']?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 202 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./num\_book\_write.php?w=u&amp;bk\_no=<?php echo $res['bk\_no']?>&amp;page=<?php echo $page?>&amp;bg\_no=<?php echo $bg\_no?>&amp;st=<?php echo $st?>&amp;sv=<?php echo $sv?>&amp;ap=<?php echo $ap?>" class="btn btn\_03">수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 203 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./sms\_write.php?bk\_no=<?php echo $res['bk\_no']?>" class="btn btn\_02">보내기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 204 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./history\_num.php?st=hs\_hp&amp;sv=<?php echo $res['bk\_hp']?>" class="btn btn\_02">내역</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 217 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./num\_book\_write.php?page=<?php echo $page?>&amp;bg\_no=<?php echo $bg\_no?>" class="btn btn\_01">번호추가</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 266 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, $\_SERVER['SCRIPT\_NAME']."?bg\_no=$bg\_no&amp;st=$st&amp;sv=$sv&amp;ap=$ap&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_file.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"> <?php echo $no\_group['bg\_name']?> (<?php echo number\_format($no\_group['bg\_count'])?>) </option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_file.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $group[$i]['bg\_no']?>"> <?php echo $group[$i]['bg\_name']?> (<?php echo number\_format($group[$i]['bg\_count'])?>) </option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_file.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"> <?php echo $no\_group['bg\_name']?> (<?php echo number\_format($no\_group['bg\_count'])?>) </option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_file.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $group[$i]['bg\_no']?>"> <?php echo $group[$i]['bg\_name']?> (<?php echo number\_format($group[$i]['bg\_count'])?>) </option>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_file\_upload.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$data = file($file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_file\_upload.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "html += \"<li class=\\\"sms5\_txt\_success\\\">등록가능 ".number\_format($result)." 건<div id=\\\"regi\_hps\\\" class=\\\"local\_desc01 local\_desc\\\"></div>\";";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_file\_upload.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "html += \"<br><span class=\\\"sms5\_txt\_success\\\">총 ".number\_format($success)." 건의 휴대폰번호 등록을 완료하였습니다.</span>\";";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_file\_upload.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "parent.document.getElementById('overlap').innerHTML += '".$dupl\_hp[$i]."<br>';\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 182 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_file\_upload.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "parent.document.getElementById('regi\_hps').innerHTML += '".$regi\_hp[$i]."<br>';\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sw" value="<?php echo $sw ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $act ?>할 그룹을 한개 이상 선택하여 주십시오.</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk<?php echo $i ?>" class="sound\_only"><?php echo $list[$i]['bg\_name'] ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="<?php echo $inputbox\_type; ?>" value="<?php echo $list[$i]['bg\_no'] ?>" id="chk<?php echo $i ?>" name="chk\_bg\_no[]">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['bg\_name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="submit" value="<?php echo $act ?>" id="btn\_submit" class="btn\_submit btn">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bk\_no" value="<?php echo $write['bk\_no']?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" id="mb\_id" value="<?php echo $write['mb\_id']?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?></caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="1"><?php echo $no\_group['bg\_name']?> (<?php echo number\_format($no\_group['bg\_count'])?> 명)</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $res['bg\_no']?>" <?php echo $res['bg\_no']==$write['bg\_no']?'selected':''?>> <?php echo $res['bg\_name']?> (<?php echo number\_format($res['bg\_count'])?> 명) </option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bk\_hp" id="bk\_hp" value="<?php echo $write['bk\_hp']?>" required class="frm\_input required">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><strong>중복됨 </strong><a href="<?php echo $href; ?>" target="\_blank"><?php echo $v['mb\_id']; ?></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="bk\_receipt" id="bk\_receipt\_1" value="1" <?php echo $write['bk\_receipt']?'checked':''?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="bk\_receipt" id="bk\_receipt\_2" value="0" <?php echo !$write['bk\_receipt']?'checked':''?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td> <?php echo $write['mb\_id'] ? '<a href="'.G5\_ADMIN\_URL.'/member\_form.php?w=u&amp;mb\_id='.$write['mb\_id'].'">'.$write['mb\_id'].'</a>' : '비회원'?> </td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td> <?php echo $write['bk\_datetime']?> </td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="bk\_memo" id="bk\_memo"><?php echo html\_purifier($write['bk\_memo']); ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./num\_book.php?<?php echo clean\_query\_string($\_SERVER['QUERY\_STRING']); ?>" class="btn btn\_02">목록</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var w = "<?php echo $w; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_book\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var bk\_no = "<?php echo $bk\_no; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (confirm("한번 삭제한 자료는 복구할 방법이 없습니다.\n\n삭제되는 그룹에 속한 자료는 '<?php echo $no\_group['bg\_name']?>'로 이동됩니다.\n\n그래도 삭제하시겠습니까?"))

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if(confirm("한번 삭제한 자료는 복구할 방법이 없습니다.\n\n삭제되는 그룹에 속한 자료는 '<?php echo $no\_group['bg\_name']?>'로 이동됩니다.\n\n그래도 삭제하시겠습니까?")) {

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="btn\_ov01"><span class="ov\_txt">건수</span><span class="ov\_num"> <?php echo $total\_count; ?>건 </span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="group<?php echo isset($res['bg\_no']) ? $res['bg\_no'] : ''; ?>" method="get" action="./num\_group\_update.php" class="local\_sch02 local\_sch">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bg\_no" value="<?php echo isset($res['bg\_no']) ? $res['bg\_no'] : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $g5['title']; ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $no\_group['bg\_name']?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($no\_group['bg\_count'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($no\_group['bg\_member'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($no\_group['bg\_nomember'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($no\_group['bg\_receipt'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($no\_group['bg\_reject'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="select\_bg\_no\_999" id="select\_bg\_no\_999" onchange="move(<?php echo $no\_group['bg\_no']?>, '<?php echo $no\_group['bg\_name']?>', this);" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bg\_no[<?php echo $i ?>]" value="<?php echo $group[$i]['bg\_no']?>" id="bg\_no\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i ?>" class="sound\_only">그룹명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk[]" value="<?php echo $i ?>" id="chk\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bg\_name\_<?php echo $i; ?>" class="sound\_only">그룹명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($group[$i]['bg\_count'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($group[$i]['bg\_member'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($group[$i]['bg\_nomember'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($group[$i]['bg\_receipt'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($group[$i]['bg\_reject'])?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="select\_bg\_no\_<?php echo $i; ?>" class="sound\_only">이동할 그룹</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<select name="select\_bg\_no[<?php echo $i ?>]" id="select\_bg\_no\_<?php echo $i; ?>" onchange="move(<?php echo $group[$i]['bg\_no']?>, '<?php echo $group[$i]['bg\_name']?>', this);" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $no\_group['bg\_no']?>"><?php echo $no\_group['bg\_name']?></option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $group[$j]['bg\_no']?>"> <?php echo $group[$j]['bg\_name']?> </option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 172 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\num\_group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./num\_book.php?bg\_no=<?php echo $group[$i]['bg\_no']?>" class="btn btn\_03">보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

회원정보 최근 업데이트 : <?php echo isset($sms5['cf\_datetime']) ? $sms5['cf\_datetime'] : ''; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sms\_byte"><span id="sms\_bytes">0</span> / <span id="sms\_max\_bytes"><?php echo ($config['cf\_sms\_type'] == 'LMS' ? 90 : 80); ?></span> byte</div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo sprintf("%02d",$i)?>"<?php echo get\_selected(date('m'), $i); ?>><?php echo sprintf("%02d",$i)?></option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo sprintf("%02d",$i)?>"<?php echo get\_selected(date('d'), $i); ?>><?php echo sprintf("%02d",$i)?></option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo sprintf("%02d",$i)?>"<?php echo get\_selected(date('H')+1, $i); ?>><?php echo sprintf("%02d",$i)?></option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo sprintf("%02d",$i)?>"><?php echo sprintf("%02d",$i)?></option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 503 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var item = "<?php echo $row['bk\_name']?> (<?php echo $row['bk\_hp']?>)";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 504 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var value = "p,<?php echo $row['bk\_no']?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 514 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "add(\"$fo\_content\");";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 534 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "add(\"$wr\_message\");\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 535 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "document.getElementById('wr\_reply').value = '{$row['wr\_reply']}';\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 552 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "hp\_list.options[hp\_list.length] = new Option('$str', '$val');\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 566 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "hp\_list.options[hp\_list.length] = new Option('$str', '$val');\n";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write\_form.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$res = sql\_fetch("select count(\*) as cnt from `{$g5['sms5\_form\_table']}` where fg\_no=0");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value=""<?php echo get\_selected('', $fg\_no); ?>> 전체 </option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="0"<?php echo get\_selected('0', $fg\_no); ?>> 미분류 (<?php echo number\_format($no\_count)?>) </option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $group[$i]['fg\_no']?>"<?php echo get\_selected($fg\_no, $group[$i]['fg\_no']);?>> <?php echo $group[$i]['fg\_name']?> (<?php echo number\_format($group[$i]['fg\_count'])?>) </option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="emo\_sch" id="emo\_sch" method="get" action="<?php echo $\_SERVER['SCRIPT\_NAME']?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fg\_no" value="<?php echo $fg\_no?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="all"<?php echo get\_selected('all', $st); ?>>제목 + 이모티콘</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="name"<?php echo get\_selected('name', $st); ?>>제목</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="content"<?php echo get\_selected('content', $st); ?>>이모티콘</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="sv" value="<?php echo $sv?>" id="sv" required class="frm\_input required" size="15">

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write\_send.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$result = sql\_query("describe `{$g5['sms5\_write\_table']}`");

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write\_send.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query("ALTER TABLE `{$g5['sms5\_write\_table']}` MODIFY wr\_message TEXT NOT NULL;", false);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write\_send.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$wr\_reply = isset($\_REQUEST['wr\_reply']) ? preg\_replace('#[^0-9\-]#', '', trim($\_REQUEST['wr\_reply'])) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 358 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write\_send.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 366 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\adm\sms\_admin\sms\_write\_send.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

location.href = 'history\_view.php?wr\_no=<?php echo $wr\_no?>';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\ajax.autosave.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$uid = isset($\_REQUEST['uid']) ? preg\_replace('/[^0-9]/', '', $\_REQUEST['uid']) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\ajax.autosave.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo autosave\_count($member['mb\_id']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\ajax.autosavedel.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo autosave\_count($member['mb\_id']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\ajax.autosavelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<id>{$row['as\_id']}</id>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\ajax.autosavelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<uid>{$row['as\_uid']}</uid>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\ajax.autosavelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<subject><![CDATA[{$subject}]]></subject>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\ajax.autosavelist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<datetime>{$datetime}</datetime>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\ajax.autosaveload.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<subject><![CDATA[{$subject}]]></subject>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\ajax.autosaveload.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<content><![CDATA[{$content}]]></content>\n";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 5 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\ajax.write.token.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$token\_case = isset($\_POST['token\_case']) ? preg\_replace('/[^0-9a-z\_]/i', '', $\_POST['token\_case']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\alert.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url = preg\_replace("/[\<\>\'\"\\\'\\\"\(\)]/", "", $url);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\alert.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url = preg\_replace('/\r\n|\r|\n|[^\x20-\x7e]/','', $url);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\alert.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

alert("<?php echo $msg; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\alert.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.location.replace("<?php echo str\_replace('&amp;', '&', $url); ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\alert.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $header2 ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\alert.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $msg2 ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\alert.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form method="post" action="<?php echo $url ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\alert.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="<?php echo htmlspecialchars($key); ?>" value="<?php echo htmlspecialchars($value); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\alert.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $url ?>">돌아가기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\alert\_close.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

alert("<?php echo $msg; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\alert\_close.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $header2 ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\alert\_close.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $msg2 ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\alert\_close.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $msg3 ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 192 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\board.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ip = preg\_replace("/([0-9]+).([0-9]+).([0-9]+).([0-9]+)/", G5\_IP\_DISPLAY, $write['wr\_ip']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 235 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\board.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "\n<!-- 사용스킨 : ".(G5\_IS\_MOBILE ? $board['bo\_mobile\_skin'] : $board['bo\_skin'])." -->\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\board\_head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo html\_purifier(stripslashes($board['bo\_mobile\_content\_head']));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\board\_head.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include ($board['bo\_include\_head']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\board\_head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo html\_purifier(stripslashes($board['bo\_content\_head']));

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\board\_tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo html\_purifier(stripslashes($board['bo\_mobile\_content\_tail']));

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\board\_tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo html\_purifier(stripslashes($board['bo\_content\_tail']));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\board\_tail.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include ($board['bo\_include\_tail']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\confirm.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url1 = isset($url1) ? preg\_replace($pattern1, "", clean\_xss\_tags($url1, 1)) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\confirm.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url1 = preg\_replace($pattern2, "", $url1);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\confirm.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url2 = isset($url2) ? preg\_replace($pattern1, "", clean\_xss\_tags($url2, 1)) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\confirm.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url2 = preg\_replace($pattern2, "", $url2);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\confirm.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url3 = isset($url3) ? preg\_replace($pattern1, "", clean\_xss\_tags($url3, 1)) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\confirm.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url3 = preg\_replace($pattern2, "", $url3);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\confirm.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.location.replace("<?php echo $url1; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\confirm.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.location.replace("<?php echo $url2; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\confirm.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $url1; ?>">확인</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\confirm.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $url2; ?>">취소</a><br><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\confirm.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $url3; ?>">돌아가기</a>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 4 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\content.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$co\_id = isset($\_GET['co\_id']) ? preg\_replace('/[^a-z0-9\_]/i', '', $\_GET['co\_id']) : 0;

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\content.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($co['co\_include\_head']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\content.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace($src, $dst, $str);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\content.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="ctt\_admin"><a href="'.G5\_ADMIN\_URL.'/contentform.php?w=u&amp;co\_id='.$co\_id.'" class="btn\_admin btn"><span class="sound\_only">내용 수정</span><i class="fa fa-cog fa-spin fa-fw"></i></a></div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\content.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="ctt\_himg" class="ctt\_img"><img src="'.G5\_DATA\_URL.'/content/'.$co\_id.'\_h" alt=""></div>';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\content.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include($skin\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\content.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="ctt\_timg" class="ctt\_img"><img src="'.G5\_DATA\_URL.'/content/'.$co\_id.'\_t" alt=""></div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\content.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<p>'.str\_replace(G5\_PATH.'/', '', $skin\_file).'이 존재하지 않습니다.</p>';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\content.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($co['co\_include\_tail']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\current\_connect.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$list[$i]['name'] = preg\_replace("/([0-9]+).([0-9]+).([0-9]+).([0-9]+)/", G5\_IP\_DISPLAY, $row['lo\_ip']);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\current\_connect.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($connect\_skin\_path.'/current\_connect.skin.php');

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\db\_table.optimize.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" OPTIMIZE TABLE `{$g5['visit\_table']}`, `{$g5['visit\_sum\_table']}` ");

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\db\_table.optimize.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" OPTIMIZE TABLE `{$g5['popular\_table']}` ");

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\db\_table.optimize.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" OPTIMIZE TABLE `{$g5['board\_new\_table']}` ");

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\db\_table.optimize.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" OPTIMIZE TABLE `{$g5['memo\_table']}` ");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\delete.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/delete.head.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\delete.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/delete.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\delete.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/delete.tail.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\delete\_all.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/delete\_all.head.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\delete\_all.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/delete\_all.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\delete\_all.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/delete\_all.tail.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\delete\_comment.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/delete\_comment.head.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\delete\_comment.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/delete\_comment.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\delete\_comment.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/delete\_comment.tail.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\download.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/download.head.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\download.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/download.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\download.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/download.tail.skin.php');

**STANDARD: Potentially Unsafe Code - fopen**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\download.php

$fp = fopen($filepath, 'rb');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\download.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fp = fopen($filepath, 'rb');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\download.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

print fread($fp, round($download\_rate \* 1024));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\email\_stop.php

MD5 Hashing algorithm.

$tmp\_md5 = md5($row['mb\_id'].$row['mb\_email'].$row['mb\_datetime']);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\faq.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($skin\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\faq.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<p>'.str\_replace(G5\_PATH.'/', '', $skin\_file).'이 존재하지 않습니다.</p>';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\formmail.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($member\_skin\_path.'/formmail.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\good.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/good.head.skin.php');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\good.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '{ "error": "' . $error . '", "count": "' . $count . '" }';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\good.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/good.tail.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\group.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

require\_once($group\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div style="float:left;<?php echo $lt\_style ?>" class="lt\_wr">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo latest('basic', $row['bo\_table'], 6, 25);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\link.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$no = isset($\_REQUEST['no']) ? preg\_replace('/[^0-9]/i', '', $\_REQUEST['no']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 223 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\list.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$qstr1 = preg\_replace($patterns, '', $qstr);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 230 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\list.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$qstr1 = preg\_replace($patterns, '', $qstr);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 255 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\list.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($board\_skin\_path.'/list.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\login.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($member\_skin\_path.'/login.skin.php');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\login\_check.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$date = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})/", "\\1년 \\2월 \\3일", $mb['mb\_intercept\_date']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\login\_check.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$date = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})/", "\\1년 \\2월 \\3일", $mb['mb\_leave\_date']);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\login\_check.php

MD5 Hashing algorithm.

$ckey = md5($mb['mb\_ip'].$mb['mb\_datetime']);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\login\_check.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($member\_skin\_path.'/login\_check.skin.php');

**MEDIUM: Potentially Unsafe Code - md5**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\login\_check.php

MD5 Hashing algorithm.

set\_session('ss\_mb\_key', md5($mb['mb\_datetime'] . get\_real\_client\_ip() . $\_SERVER['HTTP\_USER\_AGENT']));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\login\_check.php

MD5 Hashing algorithm.

$key = md5($\_SERVER['SERVER\_ADDR'] . $\_SERVER['SERVER\_SOFTWARE'] . $\_SERVER['HTTP\_USER\_AGENT'] . $mb['mb\_password']);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\login\_check.php

$tmp\_data\_check = @fopen($tmp\_data\_file, 'w');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\login\_check.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$tmp\_data\_check = @fopen($tmp\_data\_file, 'w');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\login\_check.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if(! @fwrite($tmp\_data\_check, G5\_URL)){

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\member\_cert\_refresh.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($member\_skin\_path.'/member\_cert\_refresh.skin.php');

**MEDIUM: Potentially Unsafe Code - md5**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\member\_cert\_refresh\_update.php

MD5 Hashing algorithm.

if ($cert\_type == 'ipin' && get\_session('ss\_cert\_hash') == md5($mb\_name.$cert\_type.get\_session('ss\_cert\_birth').$md5\_cert\_no)) {

**MEDIUM: Potentially Unsafe Code - md5**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\member\_cert\_refresh\_update.php

MD5 Hashing algorithm.

} else if($cert\_type != 'ipin' && get\_session('ss\_cert\_hash') == md5($mb\_name.$cert\_type.get\_session('ss\_cert\_birth').$mb\_hp.$md5\_cert\_no)) {

**MEDIUM: Potentially Unsafe Code - md5**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\member\_cert\_refresh\_update.php

MD5 Hashing algorithm.

if($cert\_type == 'ipin' && get\_session('ss\_cert\_hash') == md5($mb\_name.$cert\_type.get\_session('ss\_cert\_birth').$md5\_cert\_no)) {

**MEDIUM: Potentially Unsafe Code - md5**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\member\_cert\_refresh\_update.php

MD5 Hashing algorithm.

}else if($cert\_type != 'ipin' && get\_session('ss\_cert\_hash') == md5($mb\_name.$cert\_type.get\_session('ss\_cert\_birth').$mb\_hp.$md5\_cert\_no)) {

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\member\_confirm.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url = preg\_replace('#^/\\\{1,}#', '/', $url);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\member\_confirm.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url = preg\_replace('#^/{3,}#', '/', $url);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\member\_confirm.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($member\_skin\_path.'/member\_confirm.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\memo.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($member\_skin\_path.'/memo.skin.php');

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\memo\_delete.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " update `{$g5['member\_table']}` set mb\_memo\_cnt = '".get\_memo\_not\_read($member['mb\_id'])."' where mb\_id = '{$member['mb\_id']}' ";

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\memo\_form.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($member\_skin\_path.'/memo\_form.skin.php');

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\memo\_view.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " update `{$g5['member\_table']}` set mb\_memo\_cnt = '".get\_memo\_not\_read($member['mb\_id'])."' where mb\_id = '{$member['mb\_id']}' ";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\memo\_view.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " select me.\*, a.rownum from `{$g5['memo\_table']}` as me inner join ( select me\_id , (@rownum:=@rownum+1) as rownum from `{$g5['memo\_table']}` as memo, (select @rownum:=0) tmp where me\_{$kind}\_mb\_id = '{$member['mb\_id']}' and memo.me\_type = '$kind' order by me\_id desc ) as a on a.me\_id = me.me\_id where me.me\_id < '$me\_id' and me.me\_{$kind}\_mb\_id = '{$member['mb\_id']}' and me.me\_type = '$kind' order by me.me\_id desc limit 1 ";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\memo\_view.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " select me.\*, a.rownum from `{$g5['memo\_table']}` as me inner join ( select me\_id , (@rownum:=@rownum+1) as rownum from `{$g5['memo\_table']}` as memo, (select @rownum:=0) tmp where me\_{$kind}\_mb\_id = '{$member['mb\_id']}' and memo.me\_type = '$kind' order by me\_id asc ) as a on a.me\_id = me.me\_id where me.me\_id > '$me\_id' and me.me\_{$kind}\_mb\_id = '{$member['mb\_id']}' and me.me\_type = '$kind' order by me.me\_id asc limit 1 ";

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\memo\_view.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($member\_skin\_path.'/memo\_view.skin.php');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$wr\_id\_val = isset($\_POST['chk\_wr\_id'][$i]) ? preg\_replace('/[^0-9]/', '', $\_POST['chk\_wr\_id'][$i]) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sw" value="<?php echo $sw ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id\_list" value="<?php echo $wr\_id\_list ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="act" value="<?php echo $act ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="url" value="<?php echo get\_text(clean\_xss\_tags($\_SERVER['HTTP\_REFERER'])); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $act ?>할 게시판을 한개 이상 선택하여 주십시오.</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $atc\_bg; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk<?php echo $i ?>" class="sound\_only"><?php echo $list[$i]['bo\_table'] ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" value="<?php echo $list[$i]['bo\_table'] ?>" id="chk<?php echo $i ?>" name="chk\_bo\_table[]">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['gr\_subject'] . ' &gt; ';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['bo\_subject'] ?> (<?php echo $list[$i]['bo\_table'] ?>)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $atc\_mark; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="submit" value="<?php echo $act ?>" id="btn\_submit" class="btn\_submit">

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$wr\_id\_list = isset($\_POST['wr\_id\_list']) ? preg\_replace('/[^0-9\,]/', '', $\_POST['wr\_id\_list']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$move\_bo\_table = isset($\_POST['chk\_bo\_table'][$i]) ? preg\_replace('/[^a-z0-9\_]/i', '', $\_POST['chk\_bo\_table'][$i]) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$copy\_file\_name = preg\_replace('/\_copy(\d+)?\_(\d+)\_/', $replace\_str, $copy\_file\_name);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 278 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move\_update.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

alert("<?php echo $msg; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 279 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move\_update.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

opener.document.location.href = "<?php echo $opener\_href1; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 284 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move\_update.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $msg; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 286 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\move\_update.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $opener\_href; ?>">돌아가기</a>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\new.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$gr\_id = isset($\_GET['gr\_id']) ? substr(preg\_replace('#[^a-z0-9\_]#i', '', $\_GET['gr\_id']), 0, 10) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\new.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$mb\_id = substr(preg\_replace('#[^a-z0-9\_]#i', '', $mb\_id), 0, 20);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\new.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($new\_skin\_path.'/new.skin.php');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\newwin.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="hd\_pops\_<?php echo $nw['nw\_id'] ?>" class="hd\_pops" style="top:<?php echo $nw['nw\_top']?>px;left:<?php echo $nw['nw\_left']?>px">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\newwin.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="hd\_pops\_con" style="width:<?php echo $nw['nw\_width'] ?>px;height:<?php echo $nw['nw\_height'] ?>px">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\newwin.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($nw['nw\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\newwin.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button class="hd\_pops\_reject hd\_pops\_<?php echo $nw['nw\_id']; ?> <?php echo $nw['nw\_disable\_hours']; ?>"><strong><?php echo $nw['nw\_disable\_hours']; ?></strong>시간 동안 다시 열람하지 않습니다.</button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\newwin.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button class="hd\_pops\_close hd\_pops\_<?php echo $nw['nw\_id']; ?>">닫기 <i class="fa fa-times" aria-hidden="true"></i></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\newwin.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<span class="sound\_only">팝업레이어 알림이 없습니다.</span>';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\new\_delete.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$bo\_table = isset($\_POST['bo\_table'][$k]) ? preg\_replace('/[^a-z0-9\_]/i', '', $\_POST['bo\_table'][$k]) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\new\_delete.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$wr\_id = isset($\_POST['wr\_id'][$k]) ? preg\_replace('/[^0-9]/i', '', $\_POST['wr\_id'][$k]) : 0;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\password.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$comment\_id = isset($\_REQUEST['comment\_id']) ? preg\_replace('/[^0-9]/', '', $\_REQUEST['comment\_id']) : 0;

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\password.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($member\_skin\_path.'/password.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\password\_lost.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($member\_skin\_path.'/password\_lost.skin.php');

**MEDIUM: Potentially Unsafe Code - md5**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\password\_lost2.php

MD5 Hashing algorithm.

$mb\_nonce = md5(pack('V\*', rand(), rand(), rand(), rand()));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\password\_lost\_certify.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$mb\_no = isset($\_GET['mb\_no']) ? preg\_replace('#[^0-9]#', '', trim($\_GET['mb\_no'])) : 0;

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\password\_reset.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($member\_skin\_path.'/password\_reset.skin.php');

**MEDIUM: Potentially Unsafe Code - Code Appears to Contain Hard-Coded Password**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\password\_reset\_update.php

The code may contain a hard-coded password which an attacker could obtain from the source or by dis-assembling the executable. Please manually review the code:

$sql\_password = "mb\_password = '".get\_encrypt\_string($mb\_password)."' ";

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\point.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($member\_skin\_path.'/point.skin.php');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\poll\_etc\_update\_mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $subject ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\poll\_etc\_update\_mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

작성자 <?php echo $name ?> (<?php echo $mb\_id ?>)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\poll\_etc\_update\_mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $content ?>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\poll\_result.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once ($poll\_skin\_path.'/poll\_result.skin.php');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 4 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\poll\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$po\_id = isset($\_POST['po\_id']) ? preg\_replace('/[^0-9]/', '', $\_POST['po\_id']) : 0;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\poll\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$gb\_poll = isset($\_POST['gb\_poll']) ? preg\_replace('/[^0-9]/', '', $\_POST['gb\_poll']) : 0;

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\profile.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($member\_skin\_path.'/profile.skin.php');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qadelete.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

goto\_url(G5\_BBS\_URL.'/qalist.php'.preg\_replace('/^&amp;/', '?', $qstr));

**STANDARD: Potentially Unsafe Code - fopen**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qadownload.php

$fp = fopen($filepath, 'rb');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qadownload.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fp = fopen($filepath, 'rb');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qadownload.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

print fread($fp, round($download\_rate \* 1024));

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qahead.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo conv\_content($qaconfig['qa\_mobile\_content\_head'], 1);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qahead.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include ($qaconfig['qa\_include\_head']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qahead.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo conv\_content($qaconfig['qa\_content\_head'], 1);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qalist.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql\_search .= " and (`{$sfl}` like '%{$stx}%') ";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qalist.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$list\_pages = preg\_replace('/(\.php)(&amp;|&)/i', '$1?', get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, './qalist.php'.$qstr.'&amp;page='));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qalist.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($skin\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div>'.str\_replace(G5\_PATH.'/', '', $skin\_file).'이 존재하지 않습니다.</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 5 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qatail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo conv\_content($qaconfig['qa\_mobile\_content\_tail'], 1);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qatail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo conv\_content($qaconfig['qa\_content\_tail'], 1);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qatail.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include ($qaconfig['qa\_include\_tail']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qaview.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$list\_href = G5\_BBS\_URL.'/qalist.php'.preg\_replace('/^&amp;/', '?', $qstr);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qaview.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($skin\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 190 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qaview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div>'.str\_replace(G5\_PATH.'/', '', $skin\_file).'이 존재하지 않습니다.</div>';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qawrite.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$list\_href = G5\_BBS\_URL.'/qalist.php'.preg\_replace('/^&amp;/', '?', $qstr);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qawrite.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($skin\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qawrite.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div>'.str\_replace(G5\_PATH.'/', '', $skin\_file).'이 존재하지 않습니다.</div>';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qawrite\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$qa\_subject = preg\_replace("#[\\\]+$#", "", $qa\_subject);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qawrite\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$qa\_content = preg\_replace("#[\\\]+$#", "", $qa\_content);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qawrite\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$qa\_hp = isset($\_POST['qa\_hp']) ? preg\_replace('/[^0-9\-]/', '', $\_POST['qa\_hp']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 220 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qawrite\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$filename = preg\_replace("/\.(php|pht|phtm|htm|cgi|pl|exe|jsp|asp|inc|phar)/i", "$0-x", $filename);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 356 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qawrite\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace('/[^0-9]/', '', $qaconfig['qa\_send\_number']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 357 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qawrite\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$recv\_number = preg\_replace('/[^0-9]/', '', $write['qa\_hp']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 385 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qawrite\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace('/[^0-9]/', '', $qaconfig['qa\_send\_number']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 386 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qawrite\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$recv\_number = preg\_replace('/[^0-9]/', '', $qaconfig['qa\_admin\_hp']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 417 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qawrite\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace('/[^0-9]/', '', $qaconfig['qa\_send\_number']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 418 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qawrite\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$recv\_number = preg\_replace('/[^0-9]/', '', $write['qa\_hp']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 431 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qawrite\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace('/[^0-9]/', '', $qaconfig['qa\_send\_number']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 432 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qawrite\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$recv\_number = preg\_replace('/[^0-9]/', '', $qaconfig['qa\_admin\_hp']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 469 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\qawrite\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$result\_url = G5\_BBS\_URL.'/qalist.php'.preg\_replace('/^&amp;/', '?', $qstr);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($member\_skin\_path.'/register.skin.php');

**MEDIUM: Potentially Unsafe Code - md5**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_email.php

MD5 Hashing algorithm.

$key = md5($mb['mb\_ip'].$mb['mb\_datetime']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_email.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $mb\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_email.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="mb\_email" id="reg\_mb\_email" required class="frm\_input email required" size="30" maxlength="100" value="<?php echo $mb['mb\_email']; ?>"></td>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_email\_update.php

MD5 Hashing algorithm.

$mb\_md5 = md5(pack('V\*', rand(), rand(), rand(), rand()));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form.php

MD5 Hashing algorithm.

$token = md5(uniqid(rand(), true));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$agree = preg\_replace('#[^0-9]#', '', $\_POST['agree']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$agree2 = preg\_replace('#[^0-9]#', '', $\_POST['agree2']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$agree = isset($\_REQUEST['agree']) ? preg\_replace('#[^0-9]#', '', $\_REQUEST['agree']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$agree2 = isset($\_REQUEST['agree2']) ? preg\_replace('#[^0-9]#', '', $\_REQUEST['agree2']) : '';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($member\_skin\_path.'/register\_form.skin.php');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$mb\_zip1 = preg\_replace('/[^0-9]/', '', $mb\_zip1);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$mb\_zip2 = preg\_replace('/[^0-9]/', '', $mb\_zip2);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($member\_skin\_path.'/register\_form\_update.head.skin.php');

**MEDIUM: Potentially Unsafe Code - md5**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update.php

MD5 Hashing algorithm.

if ($cert\_type == 'ipin' && get\_session('ss\_cert\_hash') == md5($mb\_name.$cert\_type.get\_session('ss\_cert\_birth').$md5\_cert\_no)) {

**MEDIUM: Potentially Unsafe Code - md5**

Line: 188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update.php

MD5 Hashing algorithm.

} else if($cert\_type != 'ipin' && get\_session('ss\_cert\_hash') == md5($mb\_name.$cert\_type.get\_session('ss\_cert\_birth').$mb\_hp.$md5\_cert\_no)) {

**MEDIUM: Potentially Unsafe Code - md5**

Line: 268 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update.php

MD5 Hashing algorithm.

$mb\_md5 = md5(pack('V\*', rand(), rand(), rand(), rand()));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 311 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update.php

MD5 Hashing algorithm.

if($cert\_type == 'ipin' && get\_session('ss\_cert\_hash') == md5($mb\_name.$cert\_type.get\_session('ss\_cert\_birth').$md5\_cert\_no)) {

**MEDIUM: Potentially Unsafe Code - md5**

Line: 313 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update.php

MD5 Hashing algorithm.

}else if($cert\_type != 'ipin' && get\_session('ss\_cert\_hash') == md5($mb\_name.$cert\_type.get\_session('ss\_cert\_birth').$mb\_hp.$md5\_cert\_no)) {

**MEDIUM: Potentially Unsafe Code - Code Appears to Contain Hard-Coded Password**

Line: 326 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update.php

The code may contain a hard-coded password which an attacker could obtain from the source or by dis-assembling the executable. Please manually review the code:

$sql\_password = " , mb\_password = '".get\_encrypt\_string($mb\_password)."' ";

**MEDIUM: Potentially Unsafe Code - md5**

Line: 375 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update.php

MD5 Hashing algorithm.

if($cert\_type == 'ipin' && get\_session('ss\_cert\_hash') == md5($mb\_name.$cert\_type.get\_session('ss\_cert\_birth').$md5\_cert\_no)) {

**MEDIUM: Potentially Unsafe Code - md5**

Line: 377 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update.php

MD5 Hashing algorithm.

}else if($cert\_type != 'ipin' && get\_session('ss\_cert\_hash') == md5($mb\_name.$cert\_type.get\_session('ss\_cert\_birth').$mb\_hp.$md5\_cert\_no)) {

**MEDIUM: Potentially Unsafe Code - md5**

Line: 506 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update.php

MD5 Hashing algorithm.

$mb\_md5 = md5(pack('V\*', rand(), rand(), rand(), rand()));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 571 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once ($member\_skin\_path.'/register\_form\_update.tail.skin.php');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 580 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<script>alert(\''.$msg.'\');</script>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update\_mail1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_URL ?>" target="\_blank"><?php echo $config['cf\_title'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update\_mail1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<b><?php echo $mb\_name ?></b> 님의 회원가입을 진심으로 축하합니다.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update\_mail1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $certify\_href ?>" target="\_blank" style="display:block;padding:30px 0;background:#484848;color:#fff;text-decoration:none;text-align:center">메일인증</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update\_mail2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_URL ?>" target="\_blank"><?php echo $config['cf\_title'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update\_mail2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<b><?php echo $mb\_name ?></b> 님께서 회원가입 하셨습니다.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update\_mail2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

회원 아이디 : <b><?php echo $mb\_id ?></b><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update\_mail2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

회원 이름 : <?php echo $mb\_name ?><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update\_mail2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

회원 닉네임 : <?php echo $mb\_nick ?><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update\_mail2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

추천인아이디 : <?php echo $mb\_recommend ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update\_mail2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_ADMIN\_URL ?>/member\_form.php?w=u&amp;mb\_id=<?php echo $mb\_id ?>" style="display:block;padding:30px 0;background:#484848;color:#fff;text-decoration:none;text-align:center">관리자에서 회원정보 확인하기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update\_mail3.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_URL ?>" target="\_blank"><?php echo $config['cf\_title'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update\_mail3.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<b><?php echo $mb\_name ?></b> 님의 E-mail 주소가 변경되었습니다.<br><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update\_mail3.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $certify\_href ?>" target="\_blank"><b><?php echo $certify\_href ?></b></a><br><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_form\_update\_mail3.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_BBS\_URL ?>/login.php" target="\_blank" style="display:block;padding:30px 0;background:#484848;color:#fff;text-decoration:none;text-align:center"><?php echo $config['cf\_title'] ?> 로그인</a>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\register\_result.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($member\_skin\_path.'/register\_result.skin.php');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\rss.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<title><?php echo specialchars\_replace($config['cf\_title'].' &gt; '.$subj1.' &gt; '.$subj2); ?></title>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\rss.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<link><?php echo specialchars\_replace(get\_pretty\_url($bo\_table)); ?></link>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\rss.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<title><?php echo specialchars\_replace($row['wr\_subject']); ?></title>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\rss.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<link><?php echo specialchars\_replace(get\_pretty\_url($bo\_table, $row['wr\_id'])); ?></link>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\rss.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<description><![CDATA[<?php echo $file ?><?php echo conv\_content($row['wr\_content'], $html) ?>]]></description>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\rss.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dc:creator><?php echo specialchars\_replace($row['wr\_name']) ?></dc:creator>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\rss.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dc:date><?php echo $date ?></dc:date>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\scrap.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($member\_skin\_path.'/scrap.skin.php');

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\scrap\_delete.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " update `{$g5['member\_table']}` set mb\_scrap\_cnt = '".get\_scrap\_totals($member['mb\_id'])."' where mb\_id = '{$member['mb\_id']}' ";

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\scrap\_popin.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($member\_skin\_path.'/scrap\_popin.skin.php');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\scrap\_popin\_update.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<script> alert(\'회원만 접근 가능합니다.\'); top.location.href = \''.str\_replace('&amp;', '&', $href).'\'; </script>';

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\scrap\_popin\_update.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " update `{$g5['member\_table']}` set mb\_scrap\_cnt = '".get\_scrap\_totals($member['mb\_id'])."' where mb\_id = '{$member['mb\_id']}' ";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\search.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$stx = preg\_replace('/\

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\search.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$srows = isset($\_GET['srows']) ? (int)preg\_replace('#[^0-9]#', '', $\_GET['srows']) : 10;

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 237 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\search.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($search\_skin\_path.'/search.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\view.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/view.head.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\view.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($board\_skin\_path.'/view.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\view.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/view.tail.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\view\_comment.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/view\_comment.head.skin.php');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\view\_comment.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$list[$i]['ip'] = preg\_replace("/([0-9]+).([0-9]+).([0-9]+).([0-9]+)/", G5\_IP\_DISPLAY, $row['wr\_ip']);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\view\_comment.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($board\_skin\_path.'/view\_comment.skin.php');

**MEDIUM: Potentially Unsafe Code - md5**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\view\_comment.php

MD5 Hashing algorithm.

echo '<script src="'.G5\_JS\_URL.'/md5.js"></script>'."\n";

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\view\_comment.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/view\_comment.tail.skin.php');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\view\_image.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$filename = isset($\_GET['fn']) ? preg\_replace('/[^A-Za-z0-9 \_ .\-\/]/', '', $\_GET['fn']) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\view\_image.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="bbs-view-image"><?php echo $img ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\view\_image.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var win\_w = <?php echo $width ?>;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\view\_image.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var win\_h = <?php echo $height ?> + 70;

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 435 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once ($board\_skin\_path.'/write.head.skin.php');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 440 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<!-- skin : '.(G5\_IS\_MOBILE ? $board['bo\_mobile\_skin'] : $board['bo\_skin']).' -->';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 441 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once ($board\_skin\_path.'/write.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 444 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once ($board\_skin\_path.'/write.tail.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write\_comment\_update.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/write\_comment\_update.head.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 350 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write\_comment\_update.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/write\_comment\_update.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 351 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write\_comment\_update.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/write\_comment\_update.tail.skin.php');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$uid = isset($\_POST['uid']) ? preg\_replace('/[^0-9]/', '', $\_POST['uid']) : 0;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$wr\_subject = preg\_replace("#[\\\]+$#", "", $wr\_subject);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$wr\_content = preg\_replace("#[\\\]+$#", "", $wr\_content);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$wr\_link1 = preg\_replace("#[\\\]+$#", "", $wr\_link1);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$wr\_link2 = preg\_replace("#[\\\]+$#", "", $wr\_link2);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write\_update.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/write\_update.head.skin.php');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 567 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write\_update.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$filename = preg\_replace("/\.(php|pht|phtm|htm|cgi|pl|exe|jsp|asp|inc|phar)/i", "$0-x", $filename);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 746 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write\_update.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/write\_update.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 747 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write\_update.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($board\_skin\_path.'/write\_update.tail.skin.php');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write\_update\_mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<title><?php echo $wr\_subject ?> 메일</title>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write\_update\_mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $wr\_subject ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write\_update\_mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

작성자 <?php echo $wr\_name ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write\_update\_mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $wr\_content ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\bbs\write\_update\_mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $link\_url ?>" style="display:block;padding:30px 0;background:#484848;color:#fff;text-decoration:none;text-align:center">사이트에서 게시물 확인하기</a>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\ajax.install.check.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$table\_prefix= isset($\_POST['table\_prefix']) ? safe\_install\_string\_check(preg\_replace('/[^a-zA-Z0-9\_]/', '\_', $\_POST['table\_prefix'])) : '';

**MEDIUM: Potentially Unsafe Code - md5**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\ajax.install.check.php

MD5 Hashing algorithm.

$ajax\_token = md5($tmp\_str.$\_SERVER['REMOTE\_ADDR'].dirname(dirname(\_\_FILE\_\_).'/'));

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\ajax.install.check.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

if(sql\_query("DESCRIBE `{$table\_prefix}config`", G5\_DISPLAY\_SQL\_ERROR, $dblink)) {

**STANDARD: Potentially Unsafe Code - system**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install.function.php

This function allows execution of commands. It is dangerous with user controlled parameters and may facilitate direct attacks against the web server.

if(preg\_match('#\);(passthru|eval|pcntl\_exec|exec|system|popen|fopen|fsockopen|file|file\_get\_contents|readfile|unlink|include|include\_once|require|require\_once)\s?#i', $str)) {

**STANDARD: Potentially Unsafe Code - exec**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install.function.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

if(preg\_match('#\);(passthru|eval|pcntl\_exec|exec|system|popen|fopen|fsockopen|file|file\_get\_contents|readfile|unlink|include|include\_once|require|require\_once)\s?#i', $str)) {

**STANDARD: Potentially Unsafe Code - popen**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install.function.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

if(preg\_match('#\);(passthru|eval|pcntl\_exec|exec|system|popen|fopen|fsockopen|file|file\_get\_contents|readfile|unlink|include|include\_once|require|require\_once)\s?#i', $str)) {

**STANDARD: Potentially Unsafe Code - passthru**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install.function.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

if(preg\_match('#\);(passthru|eval|pcntl\_exec|exec|system|popen|fopen|fsockopen|file|file\_get\_contents|readfile|unlink|include|include\_once|require|require\_once)\s?#i', $str)) {

**STANDARD: Potentially Unsafe Code - pcntl\_exec**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install.function.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

if(preg\_match('#\);(passthru|eval|pcntl\_exec|exec|system|popen|fopen|fsockopen|file|file\_get\_contents|readfile|unlink|include|include\_once|require|require\_once)\s?#i', $str)) {

**STANDARD: Potentially Unsafe Code - eval**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install.function.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

if(preg\_match('#\);(passthru|eval|pcntl\_exec|exec|system|popen|fopen|fsockopen|file|file\_get\_contents|readfile|unlink|include|include\_once|require|require\_once)\s?#i', $str)) {

**STANDARD: Potentially Unsafe Code - fopen**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install.function.php

if(preg\_match('#\);(passthru|eval|pcntl\_exec|exec|system|popen|fopen|fsockopen|file|file\_get\_contents|readfile|unlink|include|include\_once|require|require\_once)\s?#i', $str)) {

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install.function.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

if(preg\_match('#\);(passthru|eval|pcntl\_exec|exec|system|popen|fopen|fsockopen|file|file\_get\_contents|readfile|unlink|include|include\_once|require|require\_once)\s?#i', $str)) {

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<title><?php echo $title; ?></title>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><?php echo $dbconfig\_file ?></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$> mkdir <?php echo G5\_DATA\_DIR ?><br /><br />

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$> chmod 705 <?php echo G5\_DATA\_DIR ?> 또는 chmod uo+rx <?php echo G5\_DATA\_DIR ?><br /><br />

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$> chmod 707 <?php echo G5\_DATA\_DIR ?> 또는 chmod uo+rwx <?php echo G5\_DATA\_DIR ?><br /><br />

**MEDIUM: Potentially Unsafe Code - md5**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_config.php

MD5 Hashing algorithm.

$ajax\_token = md5($tmp\_str.$\_SERVER['REMOTE\_ADDR'].dirname(dirname(\_\_FILE\_\_).'/'));

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_config.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ajax\_token" value="<?php echo $ajax\_token; ?>" >

**STANDARD: Potentially Unsafe Code - system**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_config.php

This function allows execution of commands. It is dangerous with user controlled parameters and may facilitate direct attacks against the web server.

var reg = /\);(passthru|eval|pcntl\_exec|exec|system|popen|fopen|fsockopen|file|file\_get\_contents|readfile|unlink|include|include\_once|require|require\_once)\s?\(\$\_(get|post|request)\s?\[.\*?\]\s?\)/gi;

**STANDARD: Potentially Unsafe Code - exec**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_config.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

var reg = /\);(passthru|eval|pcntl\_exec|exec|system|popen|fopen|fsockopen|file|file\_get\_contents|readfile|unlink|include|include\_once|require|require\_once)\s?\(\$\_(get|post|request)\s?\[.\*?\]\s?\)/gi;

**STANDARD: Potentially Unsafe Code - popen**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_config.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

var reg = /\);(passthru|eval|pcntl\_exec|exec|system|popen|fopen|fsockopen|file|file\_get\_contents|readfile|unlink|include|include\_once|require|require\_once)\s?\(\$\_(get|post|request)\s?\[.\*?\]\s?\)/gi;

**STANDARD: Potentially Unsafe Code - passthru**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_config.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

var reg = /\);(passthru|eval|pcntl\_exec|exec|system|popen|fopen|fsockopen|file|file\_get\_contents|readfile|unlink|include|include\_once|require|require\_once)\s?\(\$\_(get|post|request)\s?\[.\*?\]\s?\)/gi;

**STANDARD: Potentially Unsafe Code - pcntl\_exec**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_config.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

var reg = /\);(passthru|eval|pcntl\_exec|exec|system|popen|fopen|fsockopen|file|file\_get\_contents|readfile|unlink|include|include\_once|require|require\_once)\s?\(\$\_(get|post|request)\s?\[.\*?\]\s?\)/gi;

**STANDARD: Potentially Unsafe Code - eval**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_config.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

var reg = /\);(passthru|eval|pcntl\_exec|exec|system|popen|fopen|fsockopen|file|file\_get\_contents|readfile|unlink|include|include\_once|require|require\_once)\s?\(\$\_(get|post|request)\s?\[.\*?\]\s?\)/gi;

**STANDARD: Potentially Unsafe Code - fopen**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_config.php

var reg = /\);(passthru|eval|pcntl\_exec|exec|system|popen|fopen|fsockopen|file|file\_get\_contents|readfile|unlink|include|include\_once|require|require\_once)\s?\(\$\_(get|post|request)\s?\[.\*?\]\s?\)/gi;

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_config.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

var reg = /\);(passthru|eval|pcntl\_exec|exec|system|popen|fopen|fsockopen|file|file\_get\_contents|readfile|unlink|include|include\_once|require|require\_once)\s?\(\$\_(get|post|request)\s?\[.\*?\]\s?\)/gi;

**STANDARD: Potentially Unsafe Code - eval**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

eval("\$file = \"$file\";");

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

eval("\$file = \"$file\";");

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$file = preg\_replace('/^--.\*$/m', '', $file);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$file = preg\_replace('/`g5\_([^`]+`)/', '`'.$table\_prefix.'$1', $file);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$file = preg\_replace('/`g5\_([^`]+`)/', '`'.$table\_prefix.'$1', $file);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$file = preg\_replace('/^--.\*$/m', '', $file);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$file = preg\_replace('/`g5\_shop\_([^`]+`)/', '`'.$g5\_shop\_prefix.'$1', $file);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$file = preg\_replace('/`g5\_shop\_([^`]+`)/', '`'.$g5\_shop\_prefix.'$1', $file);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " insert into `{$table\_prefix}config`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 223 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " insert into `{$table\_prefix}qa\_config`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 230 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " insert into `{$table\_prefix}member`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 247 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" insert into `{$table\_prefix}content` set co\_id = 'company', co\_html = '1', co\_subject = '회사소개', co\_content= '<p align=center><b>회사소개에 대한 내용을 입력하십시오.</b></p>', co\_skin = 'basic', co\_mobile\_skin = 'basic' ", true, $dblink);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 248 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" insert into `{$table\_prefix}content` set co\_id = 'privacy', co\_html = '1', co\_subject = '개인정보 처리방침', co\_content= '<p align=center><b>개인정보 처리방침에 대한 내용을 입력하십시오.</b></p>', co\_skin = 'basic', co\_mobile\_skin = 'basic' ", true, $dblink);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 249 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" insert into `{$table\_prefix}content` set co\_id = 'provision', co\_html = '1', co\_subject = '서비스 이용약관', co\_content= '<p align=center><b>서비스 이용약관에 대한 내용을 입력하십시오.</b></p>', co\_skin = 'basic', co\_mobile\_skin = 'basic' ", true, $dblink);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 252 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" insert into `{$table\_prefix}faq\_master` set fm\_id = '1', fm\_subject = '자주하시는 질문' ", true, $dblink);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 261 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" insert into `{$table\_prefix}group` set gr\_id = '$tmp\_gr\_id', gr\_subject = '$tmp\_gr\_subject' ", true, $dblink);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 270 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " insert into `{$table\_prefix}board`

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 346 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sql = preg\_replace($source, $target, $sql);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 367 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " insert into `{$g5\_shop\_prefix}default`

**STANDARD: Potentially Unsafe Code - fopen**

Line: 562 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

$f = @fopen($file, 'a');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 562 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$f = @fopen($file, 'a');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 564 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "<?php\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 565 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "if (!defined('\_GNUBOARD\_')) exit;\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 566 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "define('G5\_MYSQL\_HOST', '".addcslashes($mysql\_host, "\\'")."');\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 567 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "define('G5\_MYSQL\_USER', '".addcslashes($mysql\_user, "\\'")."');\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 568 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "define('G5\_MYSQL\_PASSWORD', '".addcslashes($mysql\_pass, "\\'")."');\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 569 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "define('G5\_MYSQL\_DB', '".addcslashes($mysql\_db, "\\'")."');\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 570 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "define('G5\_MYSQL\_SET\_MODE', {$mysql\_set\_mode});\n\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 571 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "define('G5\_TABLE\_PREFIX', '{$table\_prefix}');\n\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 572 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['write\_prefix'] = G5\_TABLE\_PREFIX.'write\_';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 573 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['auth\_table'] = G5\_TABLE\_PREFIX.'auth';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 574 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['config\_table'] = G5\_TABLE\_PREFIX.'config';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 575 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['group\_table'] = G5\_TABLE\_PREFIX.'group';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 576 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['group\_member\_table'] = G5\_TABLE\_PREFIX.'group\_member';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 577 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['board\_table'] = G5\_TABLE\_PREFIX.'board';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 578 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['board\_file\_table'] = G5\_TABLE\_PREFIX.'board\_file';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 579 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['board\_good\_table'] = G5\_TABLE\_PREFIX.'board\_good';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 580 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['board\_new\_table'] = G5\_TABLE\_PREFIX.'board\_new';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 581 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['login\_table'] = G5\_TABLE\_PREFIX.'login';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 582 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['mail\_table'] = G5\_TABLE\_PREFIX.'mail';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 583 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['member\_table'] = G5\_TABLE\_PREFIX.'member';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 584 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['memo\_table'] = G5\_TABLE\_PREFIX.'memo';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 585 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['poll\_table'] = G5\_TABLE\_PREFIX.'poll';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 586 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['poll\_etc\_table'] = G5\_TABLE\_PREFIX.'poll\_etc';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 587 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['point\_table'] = G5\_TABLE\_PREFIX.'point';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 588 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['popular\_table'] = G5\_TABLE\_PREFIX.'popular';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 589 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['scrap\_table'] = G5\_TABLE\_PREFIX.'scrap';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 590 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['visit\_table'] = G5\_TABLE\_PREFIX.'visit';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 591 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['visit\_sum\_table'] = G5\_TABLE\_PREFIX.'visit\_sum';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 592 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['uniqid\_table'] = G5\_TABLE\_PREFIX.'uniqid';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 593 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['autosave\_table'] = G5\_TABLE\_PREFIX.'autosave';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 594 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['cert\_history\_table'] = G5\_TABLE\_PREFIX.'cert\_history';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 595 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['qa\_config\_table'] = G5\_TABLE\_PREFIX.'qa\_config';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 596 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['qa\_content\_table'] = G5\_TABLE\_PREFIX.'qa\_content';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 597 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['content\_table'] = G5\_TABLE\_PREFIX.'content';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 598 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['faq\_table'] = G5\_TABLE\_PREFIX.'faq';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 599 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['faq\_master\_table'] = G5\_TABLE\_PREFIX.'faq\_master';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 600 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['new\_win\_table'] = G5\_TABLE\_PREFIX.'new\_win';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 601 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['menu\_table'] = G5\_TABLE\_PREFIX.'menu';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 602 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['social\_profile\_table'] = G5\_TABLE\_PREFIX.'member\_social\_profiles';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 603 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['member\_cert\_history\_table'] = G5\_TABLE\_PREFIX.'member\_cert\_history';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 606 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 607 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "define('G5\_USE\_SHOP', true);\n\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 608 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "define('G5\_SHOP\_TABLE\_PREFIX', '{$g5\_shop\_prefix}');\n\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 609 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_default\_table'] = G5\_SHOP\_TABLE\_PREFIX.'default';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 610 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_banner\_table'] = G5\_SHOP\_TABLE\_PREFIX.'banner';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 611 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_cart\_table'] = G5\_SHOP\_TABLE\_PREFIX.'cart';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 612 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_category\_table'] = G5\_SHOP\_TABLE\_PREFIX.'category';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 613 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_event\_table'] = G5\_SHOP\_TABLE\_PREFIX.'event';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 614 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_event\_item\_table'] = G5\_SHOP\_TABLE\_PREFIX.'event\_item';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 615 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_item\_table'] = G5\_SHOP\_TABLE\_PREFIX.'item';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 616 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_item\_option\_table'] = G5\_SHOP\_TABLE\_PREFIX.'item\_option';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 617 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_item\_use\_table'] = G5\_SHOP\_TABLE\_PREFIX.'item\_use';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 618 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_item\_qa\_table'] = G5\_SHOP\_TABLE\_PREFIX.'item\_qa';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 619 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_item\_relation\_table'] = G5\_SHOP\_TABLE\_PREFIX.'item\_relation';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 620 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_order\_table'] = G5\_SHOP\_TABLE\_PREFIX.'order';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 621 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_order\_delete\_table'] = G5\_SHOP\_TABLE\_PREFIX.'order\_delete';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 622 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_wish\_table'] = G5\_SHOP\_TABLE\_PREFIX.'wish';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 623 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_coupon\_table'] = G5\_SHOP\_TABLE\_PREFIX.'coupon';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 624 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_coupon\_zone\_table'] = G5\_SHOP\_TABLE\_PREFIX.'coupon\_zone';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 625 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_coupon\_log\_table'] = G5\_SHOP\_TABLE\_PREFIX.'coupon\_log';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 626 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_sendcost\_table'] = G5\_SHOP\_TABLE\_PREFIX.'sendcost';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 627 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_personalpay\_table'] = G5\_SHOP\_TABLE\_PREFIX.'personalpay';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 628 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_order\_address\_table'] = G5\_SHOP\_TABLE\_PREFIX.'order\_address';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 629 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_item\_stocksms\_table'] = G5\_SHOP\_TABLE\_PREFIX.'item\_stocksms';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 630 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_post\_log\_table'] = G5\_SHOP\_TABLE\_PREFIX.'order\_post\_log';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 631 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_order\_data\_table'] = G5\_SHOP\_TABLE\_PREFIX.'order\_data';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 632 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "\$g5['g5\_shop\_inicis\_log\_table'] = G5\_SHOP\_TABLE\_PREFIX.'inicis\_log';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 635 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, "?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 641 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li>DB설정 파일 생성 완료 (<?php echo $file ?>)</li>

**STANDARD: Potentially Unsafe Code - fopen**

Line: 645 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

$f = fopen($data\_path.'/.htaccess', 'w');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 645 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$f = fopen($data\_path.'/.htaccess', 'w');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 652 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\install\install\_db.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($f, $str);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\cache.lib.php

MD5 Hashing algorithm.

$str = substr(md5($\_SERVER['SERVER\_SOFTWARE'].$\_SERVER['DOCUMENT\_ROOT']), 0, 6);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url = preg\_replace('#(&amp;)?page=[0-9]\*#', '', $url);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace("/^(<nav[^>]+><span[^>]+>)/", '$1'.$insert\_html.PHP\_EOL, $paging\_html);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace("#(</span></nav>)$#", $php\_eol.$insert\_html.'$1', $paging\_html);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

print\_r($var);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo nl2br("<span style='font-family:Tahoma, 굴림; font-size:9pt;'>$str</span>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'location.replace("'.$url.'");';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<meta http-equiv="refresh" content="0;url='.$url.'" />';

**MEDIUM: Potentially Unsafe Code - md5**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

MD5 Hashing algorithm.

setcookie(md5($cookie\_name), base64\_encode($value), G5\_SERVER\_TIME + $expire, '/', G5\_COOKIE\_DOMAIN);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

MD5 Hashing algorithm.

$cookie = md5($cookie\_name);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 241 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace("/([^(href=\"?'?)|(src=\"?'?)]|\(|^)((http|https|ftp|telnet|news|mms):\/\/[a-zA-Z0-9\.-]+\.[가-힣\xA1-\xFEa-zA-Z0-9\.:&#!=\_\?\/~\+%@;\-\|\,\(\)]+)/i", "\\1<A HREF=\"\\2\" TARGET=\"{$config['cf\_link\_target']}\" $attr\_nofollow>\\2</A>", $str);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 242 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace("/(^|[\"'\s(])(www\.[^\"'\s()]+)/i", "\\1<A HREF=\"http://\\2\" TARGET=\"{$config['cf\_link\_target']}\" $attr\_nofollow>\\2</A>", $str);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 243 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace("/[0-9a-z\_-]+@[a-z0-9.\_-]{4,}/i", "<a href=\"mailto:\\0\" $attr\_nofollow>\\0</a>", $str);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 513 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace("/($pattern)/i", $replace, $str);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 549 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$content = preg\_replace($source, $target, $content);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 719 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$wr\_bo\_table = preg\_replace('/^'.preg\_quote($g5['write\_prefix']).'/i', '', $write\_table);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 755 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$gr\_id = preg\_replace('/[^a-z0-9\_]/i', '', $gr\_id);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 757 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

MD5 Hashing algorithm.

$key = md5($gr\_id);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 782 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

MD5 Hashing algorithm.

$key = md5($fields);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1427 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace("/>$/", " $attribute>", $view['file'][$number]['view']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1514 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace("/\&([a-z0-9]{1,20}|\#[0-9]{0,3});/i", "&#038;\\1;", $str);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1592 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sql = preg\_replace("#^select.\*from.\*[\s\(]+union[\s\)]+.\*#i ", "select 1", $sql);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1594 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sql = preg\_replace("#^select.\*from.\*where.\*`?information\_schema`?.\*#i", "select 1", $sql);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 1716 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " select \* from `$table` limit 1 ";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1781 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$schema\_create = preg\_replace('/,' . $crlf . '$/', '', $schema\_create);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 2036 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $q;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 2039 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo " <font color=blue>(type={$row['type']} , key={$row['key']})</font>";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2055 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace("/\<([\/]?)(script|iframe|form)([^\>]\*)\>?/i", "&lt;$1$2$3&gt;", $code);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 2065 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

MD5 Hashing algorithm.

return md5(uniqid(rand(), true));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 2072 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

MD5 Hashing algorithm.

$token = md5(uniqid(rand(), true));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace( '/(([\x80-\xff]{3})\*?)([\x80-\xff]{0,2})$/', '$1', $str );

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2311 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fn = preg\_replace("/\.[^\.]+$/i", "", basename($file));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2355 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$filename = preg\_replace("/\.[^\.]+$/i", "", basename($srcfile));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2357 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$files = glob($filepath.'/thumb-'.$filename.'\*');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2373 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$fn = preg\_replace("/\.[^\.]+$/i", "", basename($file));

**STANDARD: Potentially Unsafe Code - fopen**

Line: 2482 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

$f = @fopen($filename, 'w');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2482 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$f = @fopen($filename, 'w');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2486 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$bytes = fwrite($f, $data);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2599 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$link[1] = preg\_replace('#\.css([\'\"]?>)$#i', '.css?ver='.G5\_CSS\_VER.'$1', $link[1]);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2628 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$js[1] = preg\_replace('#\.js([\'\"]?>)<\/script>$#i', '.js'.$add\_version\_str.'$1</script>', $js[1]);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2640 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$buffer = preg\_replace('#(</title>[^<]\*<link[^>]+>)#', "$1$stylesheet", $buffer);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2650 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$buffer = preg\_replace('#(</head>[^<]\*<body[^>]\*>)#', "$javascript{$nl}$1", $buffer);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2660 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$buffer = preg\_replace('#(<title[^>]\*>.\*?</title>)#', "$meta\_tag{$nl}$1", $buffer);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2670 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$hp = preg\_replace("/[^0-9]/", "", $hp);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2671 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace("/([0-9]{3})([0-9]{3,4})([0-9]{4})$/", "\\1-\\2-\\3", $hp);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 2779 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['member\_cert\_history\_table']}` (

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 2880 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "$errstr ($errno)\n";

**STANDARD: Potentially Unsafe Code - exec**

Line: 2928 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

if ( !function\_exists('exec') ) {

**STANDARD: Potentially Unsafe Code - exec**

Line: 2929 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

alert('exec 함수실행이 불가능하므로 사용할수 없습니다.');

**STANDARD: Potentially Unsafe Code - exec**

Line: 2938 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

exec($exe.' -h 2>&1', $out, $return\_var);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 2938 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

exec($exe.' -h 2>&1', $out, $return\_var);

**STANDARD: Potentially Unsafe Code - exec**

Line: 2953 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

exec($exe.' -h 2>&1', $out, $return\_var);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 2953 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

exec($exe.' -h 2>&1', $out, $return\_var);

**STANDARD: Potentially Unsafe Code - exec**

Line: 2968 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

exec($exe.' D 2>&1', $out, $return\_var);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 2968 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

exec($exe.' D 2>&1', $out, $return\_var);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 3071 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$stx = preg\_replace($stx\_pattern, $stx\_replace, $stx);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 3091 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$result = preg\_replace('#<

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 3610 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$this->salt = md5(preg\_replace('/[^0-9A-Za-z]/', substr(G5\_MYSQL\_USER, -1), $\_SERVER['SERVER\_SOFTWARE'].$\_SERVER['DOCUMENT\_ROOT']));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 3610 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

MD5 Hashing algorithm.

$this->salt = md5(preg\_replace('/[^0-9A-Za-z]/', substr(G5\_MYSQL\_USER, -1), $\_SERVER['SERVER\_SOFTWARE'].$\_SERVER['DOCUMENT\_ROOT']));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 3651 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

MD5 Hashing algorithm.

$token = md5(uniqid(rand(), true));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 3780 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace('/[^0-9 \_\-:]/i', '', $str);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 3783 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace('/[^0-9a-z\_\-]/i', '', $str);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 3794 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace('/[^0-9.]/', '', $real\_ip);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 3822 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\common.lib.php

MD5 Hashing algorithm.

$key = md5(serialize($args));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\connect.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once ($connect\_skin\_path.'/connect.skin.php');

**STANDARD: Potentially Unsafe Code - fopen**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\etc.lib.php

$fp = fopen($file, "a+");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\etc.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fp = fopen($file, "a+");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\etc.lib.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

print\_r($log);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\etc.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($fp, $msg);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\get\_data.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$co\_id = preg\_replace('/[^a-z0-9\_]/i', '', $co\_id);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\get\_data.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$bo\_table = preg\_replace('/[^a-z0-9\_]/i', '', $bo\_table);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\get\_data.lib.php

MD5 Hashing algorithm.

$key = md5($bo\_table);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\get\_data.lib.php

MD5 Hashing algorithm.

$key = md5($use\_mobile);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\get\_data.lib.php

MD5 Hashing algorithm.

$key = md5($write\_table.'|'.$where\_field.'|'.$where\_value);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 175 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\get\_data.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$wr\_bo\_table = preg\_replace('/^'.preg\_quote($g5['write\_prefix']).'/i', '', $write\_table);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 191 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\get\_data.lib.php

MD5 Hashing algorithm.

$key = md5($bo\_table.'|'.$wr\_id.$fields.$add\_where);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 211 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\get\_data.lib.php

MD5 Hashing algorithm.

$key = md5($po\_id);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 230 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\get\_data.lib.php

MD5 Hashing algorithm.

$key = md5($po\_id);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 249 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\get\_data.lib.php

MD5 Hashing algorithm.

$key = md5($ma\_id);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 268 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\get\_data.lib.php

MD5 Hashing algorithm.

$key = md5($qa\_id);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 303 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\get\_data.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return $g5['write\_prefix'].preg\_replace('/[^a-z0-9\_]/i', '', $bo\_table);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 320 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\get\_data.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sql\_str = preg\_replace('/ENGINE=MyISAM/', 'ENGINE='.G5\_DB\_ENGINE, $sql\_str);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 322 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\get\_data.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sql\_str = preg\_replace('/ENGINE=MyISAM/', '', $sql\_str);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 326 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\get\_data.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sql\_str = preg\_replace('/CHARSET=utf8/', 'CHARACTER SET '.get\_db\_charset(G5\_DB\_CHARSET), $sql\_str);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\icode.lms.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$strData = preg\_replace("/\r\n/","\n",$strData);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\icode.lms.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$strData = preg\_replace("/\r/","\n",$strData);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 294 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\icode.lms.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$strDest[$i] = preg\_replace("/[^0-9]/","",$strDest[$i]);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 308 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\icode.lms.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$\_callback = preg\_replace('/[^0-9]/', '', $callback);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 328 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\icode.lms.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$strDate = preg\_replace("/[^0-9]/", "", $strDate);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\icode.sms.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$dest=preg\_replace("/[^0-9]/i","",$dest);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\icode.sms.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$rsvTime=preg\_replace("/[^0-9]/i","",$rsvTime);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\icode.sms.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$msg = preg\_replace("/\r\n/", "\n", $msg);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\icode.sms.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$msg = preg\_replace("/\r/", "\n", $msg);

**STANDARD: Potentially Unsafe Code - eval**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\json.lib.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

eval($out . ';');

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\json.lib.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

eval($out . ';');

**STANDARD: Potentially Unsafe Code - tmpfile**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\mailer.lib.php

$tmpfile = array("name" => $filename, "path" => $dest\_file);

**STANDARD: Potentially Unsafe Code - tmpfile**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\mailer.lib.php

return $tmpfile;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\naverpay.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

if ($total\_price < preg\_replace('/[^0-9]/', '', $send\_cost\_limit[$k])) {

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\naverpay.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$diff\_cost = preg\_replace('/[^0-9]/', '', $send\_cost\_list[$k]);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 213 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\naverpay.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url = preg\_replace('#^https:#', '', $url);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\pbkdf2.compat.php

} elseif (@file\_exists('/dev/urandom') && $fp = @fopen('/dev/urandom', 'r')) {

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\pbkdf2.compat.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$salt .= pack('S', mt\_rand(0, 65535));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\poll.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once ($poll\_skin\_path.'/poll.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\popular.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once ($popular\_skin\_path.'/popular.skin.php');

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\register.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " select count(\*) as cnt from `{$g5['member\_table']}` where mb\_id = '$reg\_mb\_id' ";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\register.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$row = sql\_fetch(" select count(\*) as cnt from `{$g5['member\_table']}` where mb\_email = '$reg\_mb\_email' and mb\_id <> '$reg\_mb\_id' ");

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\register.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$reg\_mb\_hp = preg\_replace("/[^0-9]/", "", $reg\_mb\_hp);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.data.lib.php

MD5 Hashing algorithm.

$add\_query\_key = $add\_query ? 'shop\_'.md5($add\_query) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.data.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$key = substr(preg\_replace('/[^0-9a-z]/i', '', $value), 0, 2);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 160 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.data.lib.php

MD5 Hashing algorithm.

$key = md5($mb\_id);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$this->list\_skin = $list\_skin ? $list\_skin : G5\_MSHOP\_SKIN\_PATH.'/'.preg\_replace('/[^A-Za-z0-9 \_ .-]/', '', $default['de\_mobile\_type'.$this->type.'\_list\_skin']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$this->list\_skin = $list\_skin ? $list\_skin : G5\_SHOP\_SKIN\_PATH.'/'.preg\_replace('/[^A-Za-z0-9 \_ .-]/', '', $default['de\_type'.$this->type.'\_list\_skin']);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 297 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql\_common = " from `{$g5['g5\_shop\_event\_item\_table']}` a left join `{$g5['g5\_shop\_item\_table']}` b on (a.it\_id = b.it\_id) ";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 301 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql\_common = " from `{$g5['g5\_shop\_item\_table']}` ";

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 341 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include($file);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 664 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$filename = preg\_replace("/\s+/", "", $filename);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 665 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$filename = preg\_replace( $pattern, "", $filename);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 669 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$filename = preg\_replace( $pattern, "", $filename);

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 678 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

usleep(mt\_rand(100, 10000));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 741 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$datetime = preg\_replace("/[ 0:-]/", "", $datetime);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 816 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $file.' 파일을 찾을 수 없습니다.';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 844 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $file.' 파일을 찾을 수 없습니다.';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 912 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace($pattern, "\\0\n", $str);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$date = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3", $date);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$date = preg\_replace("/-/", "", $date);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1209 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<p>'.str\_replace(G5\_PATH.'/', '', $skin\_path).'파일이 존재하지 않습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $file.' 파일을 찾을 수 없습니다.';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1265 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$goods['full\_name'] = preg\_replace ("/[ #\&\+\-%@=\/\\\:;,\.'\"\^`~\\_|\!\?\\*$#<>()\[\]\{\}]/i", "", $goods['full\_name']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1338 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "alert(\"$msg\");";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1339 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "opener.location.href=\"$url\";";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1399 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$tmp\_cart\_id = preg\_replace('/[^a-z0-9\_\-]/i', '', get\_cookie('ck\_guest\_cart\_id'));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1543 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$filename = preg\_replace("/\.[^\.]+$/i", "", $file);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1545 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$files = glob($dir.'/thumb-'.$filename.'\*');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1573 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace("/([0-9A-Z]{4})([0-9A-Z]{4})([0-9A-Z]{4})([0-9A-Z]{4})/", "\\1-\\2-\\3-\\4", $str);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1804 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

if ($total\_price < preg\_replace('/[^0-9]/', '', $send\_cost\_limit[$k])) {

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1805 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_cost = preg\_replace('/[^0-9]/', '', $send\_cost\_list[$k]);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1879 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

if ($price < preg\_replace('/[^0-9]/', '', $send\_cost\_limit[$k])) {

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1880 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sendcost = preg\_replace('/[^0-9]/', '', $send\_cost\_list[$k]);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1939 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$it\_id = preg\_replace('/[^a-z0-9\_\-]/i', '', $it\_id);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 1940 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

MD5 Hashing algorithm.

$key = md5($it\_id);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2293 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_id = preg\_replace('/[^0-9a-z\_-]/i', '', clean\_xss\_tags($od\_id));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 2325 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

MD5 Hashing algorithm.

$hash\_data = md5($pp['pp\_id'].$pp['pp\_price'].$pp['pp\_time']);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 2331 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

MD5 Hashing algorithm.

$uid = md5($pp['pp\_id'].$pp['pp\_time'].$od\_ip);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 2345 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

MD5 Hashing algorithm.

$uid = md5($oid.$od\_time.$od\_ip);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2410 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$data\_path = preg\_replace('/^\/.\*\/'.G5\_DATA\_DIR.'/', '/'.G5\_DATA\_DIR, $p['path']);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 2500 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " select \* from `{$g5['g5\_shop\_cart\_table']}` where od\_id = '$s\_cart\_id' {$select\_where\_add} ";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 2563 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$conditions[] = "`{$column}` = '{$value}'";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 2567 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql\_query = "update `{$g5['g5\_shop\_cart\_table']}` set {$col\_querys} where it\_id = '{$it['it\_id']}' and od\_id = '$s\_cart\_id' and ct\_id = '{$row['ct\_id']}' ";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 2656 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$result = sql\_query("describe `{$g5['g5\_shop\_post\_log\_table']}`");

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 2659 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query("ALTER TABLE `{$g5['g5\_shop\_post\_log\_table']}` MODIFY ol\_msg TEXT NOT NULL;", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 2660 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query("ALTER TABLE `{$g5['g5\_shop\_post\_log\_table']}` DROP PRIMARY KEY;", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 2661 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query("ALTER TABLE `{$g5['g5\_shop\_post\_log\_table']}` ADD `log\_id` int(11) NOT NULL AUTO\_INCREMENT, ADD PRIMARY KEY (`log\_id`);", false);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 2667 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = "insert into `{$g5['g5\_shop\_post\_log\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 2680 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" CREATE TABLE IF NOT EXISTS `{$g5['g5\_shop\_post\_log\_table']}` (

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2711 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$tid = preg\_replace('/[^A-Za-z0-9\_\-]/', '', get\_session('P\_TID'));

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 2712 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = "select P\_TID from `{$g5['g5\_shop\_inicis\_log\_table']}` where P\_TID = '$tid' and P\_STATUS = 'cancel' ";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.uri.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$add\_query = preg\_replace("/\&amp;/", "?", $query\_string, 1);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 183 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.uri.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " SHOW COLUMNS FROM `{$g5['g5\_shop\_item\_table']}` LIKE 'it\_seo\_title' ";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.uri.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query("ALTER TABLE `{$g5['g5\_shop\_item\_table']}`

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 221 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\shop.uri.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " update `{$g5['g5\_shop\_item\_table']}` set it\_seo\_title = '{$it\_seo\_title}' where it\_id = '{$item['it\_id']}' ";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\thumbnail.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$data\_path = preg\_replace('/^\/.\*\/'.G5\_DATA\_DIR.'/', '/'.G5\_DATA\_DIR, $p['path']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\thumbnail.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$data\_path = preg\_replace('/^\/.\*\/'.G5\_DATA\_DIR.'/', '/'.G5\_DATA\_DIR, $p['path']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 268 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\thumbnail.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$thumb\_filename = preg\_replace("/\.[^\.]+$/i", "", $filename);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 725 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\thumbnail.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$contents = file\_get\_contents($filename);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 741 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\thumbnail.lib.php

MD5 Hashing algorithm.

$key = md5($filename);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 747 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\thumbnail.lib.php

if(!($fh = @fopen($filename, 'rb'))){

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 747 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\thumbnail.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if(!($fh = @fopen($filename, 'rb'))){

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\uri.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$add\_query = preg\_replace("/\&amp;/", "?", $query\_string, 1);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\uri.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

if( stripos(preg\_replace('/^https?:/i', '', $string\_url), preg\_replace('/^https?:/i', '', G5\_BBS\_URL)) === false || ! in\_array($page\_name, $array\_page\_names) ){

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 220 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\uri.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$string = preg\_replace('#'.$key.'#iu', $val, $string);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 232 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\uri.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sql\_id = preg\_replace('/[^a-z0-9\_\-]/i', '', $sql\_id);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 288 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\uri.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " update `{$db\_table}` set wr\_seo\_title = '{$wr\_seo\_title}' where wr\_id = '{$pk\_id}' ";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 297 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\uri.lib.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " update `{$db\_table}` set co\_seo\_title = '{$co\_seo\_title}' where co\_id = '{$pk\_id}' ";

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 379 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\uri.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$code = file\_get\_contents($save\_path);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 404 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\uri.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$code = file\_get\_contents($save\_path);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 411 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\uri.lib.php

$fp = fopen($save\_path, "ab");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 411 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\uri.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fp = fopen($save\_path, "ab");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 416 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\uri.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $fp, "\n" );

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 417 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\uri.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $fp, $rewrite\_str );

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 418 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\uri.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $fp, "\n" );

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\visit.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once ($visit\_skin\_path.'/visit.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Cache\FileCache.class.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$file\_contents = file\_get\_contents($cache\_file\_path);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Cache\FileCache.class.php

if ( ! $fp = @fopen($path, $mode))

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Cache\FileCache.class.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if ( ! $fp = @fopen($path, $mode))

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Cache\FileCache.class.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (($result = fwrite($fp, substr($data, $written))) === FALSE)

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\oleread.inc.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$this->data = @file\_get\_contents($sFileName);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1033 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\reader.php

64 bit floating point value. The other 34 bits are assumed to be 0

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 331 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_format.inc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$key = preg\_replace('/ /', '\_', $key); # Convert the key to a single word

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 550 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_format.inc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$key = preg\_replace('/^-/', '', $key);

**STANDARD: Potentially Unsafe Code - eval**

Line: 563 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_format.inc.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

eval("\$this->set\_$value();");

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 563 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_format.inc.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

eval("\$this->set\_$value();");

**STANDARD: Potentially Unsafe Code - eval**

Line: 565 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_format.inc.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

eval("\$this->set\_$key('$value');");

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 565 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_format.inc.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

eval("\$this->set\_$key('$value');");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_formula.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

print "$formula\n";

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 591 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_formula.inc.php

TODO: use real error codes

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 672 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_formula.inc.php

TODO: use real error codes

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 699 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_formula.inc.php

TODO: use real error codes

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 796 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_formula.inc.php

TODO: use real error codes

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 850 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_formula.inc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ext\_ref = preg\_replace("/^'/", '', $ext\_ref);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 851 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_formula.inc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ext\_ref = preg\_replace("/'$/", '', $ext\_ref);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_olewriter.inc.php

$fh = fopen($OLEfile, "wb");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_olewriter.inc.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fh = fopen($OLEfile, "wb");

**STANDARD: Potentially Unsafe Code - fopen**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_olewriter.inc.php

$fh = fopen($this->\_OLEtmpfilename, "rb");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_olewriter.inc.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fh = fopen($this->\_OLEtmpfilename, "rb");

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_workbook.inc.php

todo: print error

**STANDARD: Potentially Unsafe Code - system**

Line: 206 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_workbook.inc.php

This function allows execution of commands. It is dangerous with user controlled parameters and may facilitate direct attacks against the web server.

# Set the date system: 0 = 1900 (the default), 1 = 1904

**STANDARD: Potentially Unsafe Code - system**

Line: 216 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_workbook.inc.php

This function allows execution of commands. It is dangerous with user controlled parameters and may facilitate direct attacks against the web server.

# Return the date system: 0 = 1900, 1 = 1904

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 241 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_workbook.inc.php

todo carp "Color index $index outside range: 8 <= index <= 64";

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 250 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_workbook.inc.php

todo carp "Color component outside range: 0 <= color <= 255";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 461 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_workbook.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$this->\_store\_externs(); # For print area and repeat rows

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 463 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_workbook.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$this->\_store\_names(); # For print area and repeat rows

**STANDARD: Potentially Unsafe Code - system**

Line: 885 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_workbook.inc.php

This function allows execution of commands. It is dangerous with user controlled parameters and may facilitate direct attacks against the web server.

# Write Excel 1904 record to indicate the date system in use.

**STANDARD: Potentially Unsafe Code - system**

Line: 891 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_workbook.inc.php

This function allows execution of commands. It is dangerous with user controlled parameters and may facilitate direct attacks against the web server.

$f1904 = $this->\_1904; # Flag for 1904 date system

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 891 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_workbook.inc.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

$f1904 = $this->\_1904; # Flag for 1904 date system

**STANDARD: Potentially Unsafe Code - fopen**

Line: 206 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_worksheet.inc.php

$fh=fopen($this->\_tmpfilename, "w+b");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 206 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_worksheet.inc.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fh=fopen($this->\_tmpfilename, "w+b");

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 219 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_worksheet.inc.php

todo warn "Unable to create temp files in $dir. Refer to set\_tempdir()".

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1348 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_worksheet.inc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$formula = preg\_replace('/^=/', "", $formula);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1429 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_worksheet.inc.php

TODO ($\_[5], $\_[6]) = ($\_[6], $\_[5]) if (ref $\_[5]);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1542 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_worksheet.inc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url = preg\_replace('s[^internal:]', '', $url);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1622 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_worksheet.inc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url = preg\_replace('[^external:]', '', $url);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1623 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_worksheet.inc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url = preg\_replace('[/]', "\\", $url);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1627 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_worksheet.inc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace('[\#]', ' - ', $url);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1750 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_worksheet.inc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url = preg\_replace('[^external:]', "", $url);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1751 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_worksheet.inc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url = preg\_replace('[/]', "\\");

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1755 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_worksheet.inc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace('[\#]', " - ", $url);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 2862 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_worksheet.inc.php

$bmp=fopen($bitmap, "rb");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2862 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\Excel\php\_writeexcel\class.writeexcel\_worksheet.inc.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$bmp=fopen($bitmap, "rb");

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 4 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Autoloader.php

As we always try to run the autoloader before anything else, we can use it to do a few

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Autoloader.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

require($pClassFilePath);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2084 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

foreach (glob($localeFileDirectory.'

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2337 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$localeFunctions = file($functionNamesFile, FILE\_IGNORE\_NEW\_LINES | FILE\_SKIP\_EMPTY\_LINES);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2362 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$localeSettings = file($configFile, FILE\_IGNORE\_NEW\_LINES | FILE\_SKIP\_EMPTY\_LINES);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2423 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$value = preg\_replace($from, $to, $value);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2432 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$formula = preg\_replace($from, $to, $formula);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 3326 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$val = preg\_replace('/\s/u', '', $val);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 300 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Comment.php

MD5 Hashing algorithm.

return md5(

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 224 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\IOFactory.php

First, lucky guess by inspecting file extension

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 275 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\IOFactory.php

If we reach here then "lucky guess" didn't give any result

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 278 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\IOFactory.php

Ignore our original guess, we know that won't work

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 760 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\ReferenceHelper.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$formulaBlock = str\_replace('\\', '', preg\_replace($cellTokens, $newCellTokens, $formulaBlock));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\RichText.php

MD5 Hashing algorithm.

return md5(

**MEDIUM: Potentially Unsafe Code - md5**

Line: 612 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style.php

MD5 Hashing algorithm.

return md5(

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 718 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Worksheet.php

There is only something to do if there are some auto-size columns

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2349 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Worksheet.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$pCoordinate = preg\_replace('/^([A-Z]+)$/', '${1}:${1}', $pCoordinate);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2352 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Worksheet.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$pCoordinate = preg\_replace('/^([0-9]+)$/', '${1}:${1}', $pCoordinate);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2355 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Worksheet.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$pCoordinate = preg\_replace('/^([A-Z]+):([A-Z]+)$/', '${1}1:${2}1048576', $pCoordinate);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2358 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Worksheet.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$pCoordinate = preg\_replace('/^([0-9]+):([0-9]+)$/', 'A${1}:XFD${2}', $pCoordinate);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 2648 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Worksheet.php

MD5 Hashing algorithm.

$this->hash = md5($this->title . $this->autoFilter . ($this->protection->isProtectionEnabled() ? 't' : 'f') . \_\_CLASS\_\_);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 203 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\APC.php

MD5 Hashing algorithm.

$newCachePrefix = substr(md5($baseUnique), 0, 8) . '.';

**MEDIUM: Potentially Unsafe Code - md5**

Line: 255 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\APC.php

MD5 Hashing algorithm.

$this->cachePrefix = substr(md5($baseUnique), 0, 8) . '.';

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 304 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\CacheBase.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$baseUnique = mt\_rand();

**MEDIUM: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 304 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\CacheBase.php

The code appears to use the mt\_rand and/or smt\_rand functions without a seed to generate pseudo-random values. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker.

$baseUnique = mt\_rand();

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\DiscISAM.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

'sz' => fwrite($this->fileHandle, serialize($this->currentObject))

**STANDARD: Potentially Unsafe Code - fopen**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\DiscISAM.php

$this->fileHandle = fopen($this->fileName, 'a+');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\DiscISAM.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$this->fileHandle = fopen($this->fileName, 'a+');

**STANDARD: Potentially Unsafe Code - fopen**

Line: 193 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\DiscISAM.php

$this->fileHandle = fopen($this->fileName, 'a+');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 193 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\DiscISAM.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$this->fileHandle = fopen($this->fileName, 'a+');

**MEDIUM: Potentially Unsafe Code - md5**

Line: 204 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\Memcache.php

MD5 Hashing algorithm.

$newCachePrefix = substr(md5($baseUnique), 0, 8) . '.';

**MEDIUM: Potentially Unsafe Code - md5**

Line: 258 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\Memcache.php

MD5 Hashing algorithm.

$this->cachePrefix = substr(md5($baseUnique), 0, 8) . '.';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\PHPTemp.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

'sz' => fwrite($this->fileHandle, serialize($this->currentObject))

**STANDARD: Potentially Unsafe Code - fopen**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\PHPTemp.php

$newFileHandle = fopen('php:

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\PHPTemp.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($newFileHandle, fread($this->fileHandle, 1024));

**STANDARD: Potentially Unsafe Code - fopen**

Line: 186 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\PHPTemp.php

$this->fileHandle = fopen('php:

**STANDARD: Potentially Unsafe Code - exec**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\SQLite.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$result = $this->DBHandle->exec($query);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\SQLite.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

$result = $this->DBHandle->exec($query);

**STANDARD: Potentially Unsafe Code - exec**

Line: 186 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\SQLite.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$result = $this->DBHandle->exec($query);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 186 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\SQLite.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

$result = $this->DBHandle->exec($query);

**STANDARD: Potentially Unsafe Code - exec**

Line: 265 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\SQLite3.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

if (!$this->DBHandle->exec('CREATE TABLE kvp\_'.$tableName.' (id VARCHAR(12) PRIMARY KEY, value BLOB)

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 265 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\SQLite3.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

if (!$this->DBHandle->exec('CREATE TABLE kvp\_'.$tableName.' (id VARCHAR(12) PRIMARY KEY, value BLOB)

**STANDARD: Potentially Unsafe Code - exec**

Line: 309 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\SQLite3.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

if (!$this->DBHandle->exec('CREATE TABLE kvp\_'.$this->TableName.' (id VARCHAR(12) PRIMARY KEY, value BLOB)')) {

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 309 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\SQLite3.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

if (!$this->DBHandle->exec('CREATE TABLE kvp\_'.$this->TableName.' (id VARCHAR(12) PRIMARY KEY, value BLOB)')) {

**STANDARD: Potentially Unsafe Code - exec**

Line: 326 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\SQLite3.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$this->DBHandle->exec('DROP TABLE kvp\_'.$this->TableName);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 326 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\SQLite3.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

$this->DBHandle->exec('DROP TABLE kvp\_'.$this->TableName);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 203 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\Wincache.php

MD5 Hashing algorithm.

$newCachePrefix = substr(md5($baseUnique), 0, 8) . '.';

**MEDIUM: Potentially Unsafe Code - md5**

Line: 257 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CachedObjectStorage\Wincache.php

MD5 Hashing algorithm.

$this->cachePrefix = substr(md5($baseUnique), 0, 8).'.';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\CalcEngine\Logger.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $cellReference,

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 497 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\DateTime.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$dateValue = preg\_replace('/(\d)(st|nd|rd|th)([ -\/])/Ui', '$1$3', $dateValue);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1356 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\Financial.php

create an initial range, with a root somewhere between 0 and guess

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 2156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\Financial.php

create an initial range, with a root somewhere between 0 and guess

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\FormulaParser.php

No attempt is made to verify formulas; assumes formulas are derived from Excel, where

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\LookupRef.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$columnKey = preg\_replace('/[^a-z]/i', '', $columnKey);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\LookupRef.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$startAddress = preg\_replace('/[^a-z]/i', '', $startAddress);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\LookupRef.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$endAddress = preg\_replace('/[^a-z]/i', '', $endAddress);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\LookupRef.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$cellAddress = preg\_replace('/[^a-z]/i', '', $cellAddress);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 199 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\LookupRef.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return (integer) preg\_replace('/[^0-9]/i', '', $rowKey);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 208 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\LookupRef.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$startAddress = preg\_replace('/[^0-9]/', '', $startAddress);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 209 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\LookupRef.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$endAddress = preg\_replace('/[^0-9]/', '', $endAddress);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 217 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\LookupRef.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return (integer) preg\_replace('/[^0-9]/', '', $cellAddress);

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 926 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\MathTrig.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

return (mt\_rand(0, 10000000)) / 10000000;

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 928 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\MathTrig.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

return mt\_rand($min, $max);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\Statistical.php

case if the initial guess is too rough) we apply a bisection

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1441 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\Statistical.php

$CumPGuessMinus1 = $CumPGuess - $PGuess;

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1707 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\Statistical.php

case if the initial guess is too rough) we apply a bisection

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 3398 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\Statistical.php

case if the initial guess is too rough) we apply a bisection

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Calculation\TextData.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return trim(preg\_replace('/ +/', ' ', trim($stringValue, ' ')), ' ');

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Cell\DataType.php

TODO: Sanitize Rich-Text string (max. character count is 32,767)

**MEDIUM: Potentially Unsafe Code - md5**

Line: 460 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Cell\DataValidation.php

MD5 Hashing algorithm.

return md5(

**MEDIUM: Potentially Unsafe Code - md5**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Cell\Hyperlink.php

MD5 Hashing algorithm.

return md5(

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 865 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Chart\Renderer\jpgraph.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $chartType.' is not yet implemented<br />';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 617 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Helper\HTML.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$text = preg\_replace('/\n \*/mu', "\n", $text);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 766 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Helper\HTML.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$domText = preg\_replace(

**STANDARD: Potentially Unsafe Code - fopen**

Line: 237 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Abstract.php

$this->fileHandle = fopen($pFilename, 'r');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 237 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Abstract.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$this->fileHandle = fopen($pFilename, 'r');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 287 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Abstract.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

return $this->securityScan(file\_get\_contents($filestream));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel2003XML.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$xml = simplexml\_load\_string($this->securityScan(file\_get\_contents($pFilename)), 'SimpleXMLElement', PHPExcel\_Settings::getLibXmlLoaderOptions());

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 160 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel2003XML.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$xml = simplexml\_load\_string($this->securityScan(file\_get\_contents($pFilename)), 'SimpleXMLElement', PHPExcel\_Settings::getLibXmlLoaderOptions());

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 324 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel2003XML.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$xml = simplexml\_load\_string($this->securityScan(file\_get\_contents($pFilename)), 'SimpleXMLElement', PHPExcel\_Settings::getLibXmlLoaderOptions());

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1416 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel2007.php

TODO: Autoshapes from twoCellAnchors!

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1550 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel2007.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$extractedRange = preg\_replace('/\'(\w+)\'\!/', '', $extractedRange);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1596 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel2007.php

FIXME: what if sheetname contains comma?

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1599 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel2007.php

FIXME: what if sheetname contains exclamation mark?

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1625 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel2007.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$extractedRange = preg\_replace('/\'(\w+)\'\!/', '', $extractedRange);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1977 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel2007.php

we need to save id and target to avoid parsing customUI.xml and "guess" if it's a pseudo callback who load the image

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2007 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel2007.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace('~[^/]+/\.\./~', '', dirname($base) . "/$add");

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

FIXME: what if sheetname contains comma?

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

FIXME: what if sheetname contains exclamation mark?

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1169 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

FIXME: what if sheetname contains comma?

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1216 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

TODO Provide support for named values

**MEDIUM: Potentially Unsafe Code - md5**

Line: 1791 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

MD5 Hashing algorithm.

$md5 = new PHPExcel\_Reader\_Excel5\_MD5();

**MEDIUM: Potentially Unsafe Code - md5**

Line: 1792 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

MD5 Hashing algorithm.

$md5->add($pwarray);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 1794 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

MD5 Hashing algorithm.

$s = $md5->getContext();

**MEDIUM: Potentially Unsafe Code - md5**

Line: 1821 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

MD5 Hashing algorithm.

$md5 = new PHPExcel\_Reader\_Excel5\_MD5();

**MEDIUM: Potentially Unsafe Code - md5**

Line: 1822 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

MD5 Hashing algorithm.

$md5->add($pwarray);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 1824 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

MD5 Hashing algorithm.

$mdContext1 = $md5->getContext();

**MEDIUM: Potentially Unsafe Code - md5**

Line: 1830 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

MD5 Hashing algorithm.

$md5->reset();

**MEDIUM: Potentially Unsafe Code - md5**

Line: 1842 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

MD5 Hashing algorithm.

$md5->add($pwarray);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 1864 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

MD5 Hashing algorithm.

$md5->add($pwarray);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 1865 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

MD5 Hashing algorithm.

$valContext = $md5->getContext();

**MEDIUM: Potentially Unsafe Code - md5**

Line: 1875 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

MD5 Hashing algorithm.

$md5->reset();

**MEDIUM: Potentially Unsafe Code - md5**

Line: 1876 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

MD5 Hashing algorithm.

$md5->add($salt);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 1877 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

MD5 Hashing algorithm.

$mdContext2 = $md5->getContext();

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 2092 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

this has to do with that index 4 is omitted in all BIFF versions for some strange reason

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 3722 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

this has to do with that index 4 is omitted in all BIFF versions for some strange reason

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 4165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

todo: what if string is very long? continue record

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 4334 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

FIXME: set $firstVisibleRow and $firstVisibleColumn

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 4470 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$selectedCells = preg\_replace('/^([A-Z]+1\:[A-Z]+)16384$/', '${1}1048576', $selectedCells);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 4475 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$selectedCells = preg\_replace('/^([A-Z]+1\:[A-Z]+)65536$/', '${1}1048576', $selectedCells);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 4480 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$selectedCells = preg\_replace('/^(A[0-9]+\:)IV([0-9]+)$/', '${1}XFD${2}', $selectedCells);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 4681 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

todo: implement

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 4944 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

TODO: Investigate structure for .xls SHEETLAYOUT record as saved by MS Office Excel 2007

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 4983 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

rgbHdrSData, assume "Enhanced Protection"

**MEDIUM: Potentially Unsafe Code - Unsafe Password Management**

Line: 5108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

The application appears to handle passwords in a case-insensitive manner. This can greatly increase the likelihood of successful brute-force and/or dictionary attacks.

$this->phpSheet->protectCells(implode(' ', $cellRanges), strtoupper(dechex($wPassword)), true);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 6744 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

assume index is to EXTERNNAME record

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 6959 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

todo: if cell range is just a single cell, should this funciton

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 7016 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

TODO: if cell range is just a single cell, should this funciton

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 7178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

todo: check if we have identified the whole set of special characters

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 7180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

and we may assume that they are not present: []\*/:\?

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 7188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

TODO: external sheet support

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 7429 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

this offset assumes richtext and Asian phonetic settings are off which is generally wrong

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 7491 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

of the 64 bit floating point value. The other 34 bits are assumed

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 7576 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Excel5.php

Hacked by Andreas Rehm 2006 to ensure correct result of the <<24 block on 32 and 64bit systems

**STANDARD: Potentially Unsafe Code - fopen**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Gnumeric.php

$fh = fopen($pFilename, 'r');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\Gnumeric.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fh = fopen($pFilename, 'r');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 233 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\HTML.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$domText = preg\_replace('/\s+/u', ' ', trim($child->nodeValue));

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 524 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\OOCalc.php

Also, here we assume there is no text data is span fields are specified, since

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 618 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\OOCalc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$value = preg\_replace('/\[([^\.]+)\.([^\.]+):\.([^\.]+)\]/Ui', '$1!$2:$3', $value);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 619 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\OOCalc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$value = preg\_replace('/\[([^\.]+)\.([^\.]+)\]/Ui', '$1!$2', $value);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 620 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\OOCalc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$value = preg\_replace('/\[\.([^\.]+):\.([^\.]+)\]/Ui', '$1:$2', $value);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 621 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Reader\OOCalc.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$value = preg\_replace('/\[\.([^\.]+)\]/Ui', '$1', $value);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\RichText\Run.php

MD5 Hashing algorithm.

return md5(

**MEDIUM: Potentially Unsafe Code - md5**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\RichText\TextElement.php

MD5 Hashing algorithm.

return md5(

**STANDARD: Potentially Unsafe Code - fopen**

Line: 181 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\Drawing.php

$file = fopen($p\_sFile, "rb");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 181 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\Drawing.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$file = fopen($p\_sFile, "rb");

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\Excel5.php

here we assume Arial 10

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 312 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\Font.php

but since GD2 seems to assume 72dpi, pixels and points are the same

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 345 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\Font.php

Calculate column width in pixels. We assume fixed glyph width. Result varies with font name and size.

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 368 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\Font.php

just assume Calibri

**STANDARD: Potentially Unsafe Code - fopen**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE.php

$fh = fopen($file, "r");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fh = fopen($file, "r");

**STANDARD: Potentially Unsafe Code - fopen**

Line: 218 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE.php

return fopen($path, 'r');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 218 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

return fopen($path, 'r');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLERead.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$this->data = file\_get\_contents($sFileName, false, null, 0, 8);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLERead.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$this->data = file\_get\_contents($sFileName);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 308 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLERead.php

Hacked by Andreas Rehm 2006 to ensure correct result of the <<24 block on 32 and 64bit systems

**MEDIUM: Potentially Unsafe Code - Unsafe Password Management**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PasswordHasher.php

The application appears to handle passwords in a case-insensitive manner. This can greatly increase the likelihood of successful brute-force and/or dictionary attacks.

return(strtoupper(dechex($password)));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\XMLWriter.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

return file\_get\_contents($this->tempFileName);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\ZipArchive.php

$handle = fopen($this->tempDir.'/'.$filenameParts["basename"], "wb");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\ZipArchive.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$handle = fopen($this->tempDir.'/'.$filenameParts["basename"], "wb");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\ZipArchive.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($handle, $contents);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

$this->\_FILEH\_ = fopen($this->\_tmp\_filename, "w+b");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$this->\_FILEH\_ = fopen($this->\_tmp\_filename, "w+b");

**STANDARD: Potentially Unsafe Code - fopen**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

$this->\_FILEH\_ = fopen($filename, "wb");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$this->\_FILEH\_ = fopen($filename, "wb");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 233 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, pack("V", $iAll+$iBdCnt) . pack("V", $iBdExL));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 238 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, pack("V", $iAll+$i));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 243 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, (pack("V", -1)));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 274 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, $raList[$i]->\_data);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 278 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, str\_repeat("\x00", $this->\_BIG\_BLOCK\_SIZE - ($raList[$i]->Size % $this->\_BIG\_BLOCK\_SIZE)));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 321 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, pack("V", $j+$iSmBlk+1));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 323 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, pack("V", -2));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 347 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, pack("V", -1));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 364 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($this->\_FILEH\_, $raList[$i]->\_getPpsWk());

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 370 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($this->\_FILEH\_, str\_repeat("\x00", ($iBCnt - ($iCnt % $iBCnt)) \* PHPExcel\_Shared\_OLE::OLE\_PPS\_SIZE));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 411 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, pack("V", $i+1));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 413 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, pack("V", -2));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 417 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, pack("V", $i+$iSbdSize+1));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 419 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, pack("V", -2));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 423 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, pack("V", $i+$iSbdSize+$iBsize+1));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 425 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, pack("V", -2));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 428 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, pack("V", 0xFFFFFFFD));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 432 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, pack("V", 0xFFFFFFFC));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 438 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, pack("V", -1));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 449 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, pack("V", $iAll+$iBdCnt+$iNb));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 451 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, pack("V", $iBsize+$iSbdSize+$iPpsCnt+$i));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 456 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, pack("V", -1));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 459 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\OLE\PPS\Root.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($FILE, pack("V", -2));

**STANDARD: Potentially Unsafe Code - fopen**

Line: 1068 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

if (($this->zip\_fd = @fopen($this->zipname, 'rb')) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1068 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (($this->zip\_fd = @fopen($this->zipname, 'rb')) == 0) {

**STANDARD: Potentially Unsafe Code - fopen**

Line: 2063 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

if (($v\_zip\_temp\_fd = @fopen($v\_zip\_temp\_name, 'wb')) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2063 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (($v\_zip\_temp\_fd = @fopen($v\_zip\_temp\_name, 'wb')) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2079 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($v\_zip\_temp\_fd, $v\_buffer, $v\_read\_size);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($this->zip\_fd, $v\_buffer, $v\_read\_size);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 2206 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

if (($this->zip\_fd = @fopen($this->zipname, $p\_mode)) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2206 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (($this->zip\_fd = @fopen($this->zipname, $p\_mode)) == 0) {

**STANDARD: Potentially Unsafe Code - fopen**

Line: 2491 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

if (($v\_file = @fopen($p\_filename, "rb")) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2491 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (($v\_file = @fopen($p\_filename, "rb")) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2527 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($this->zip\_fd, $v\_content, $p\_header['compressed\_size']);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2558 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($this->zip\_fd, $v\_content, $p\_header['compressed\_size']);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 2618 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

if (($v\_file = @fopen($p\_filename, "rb")) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2618 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (($v\_file = @fopen($p\_filename, "rb")) == 0) {

**STANDARD: Potentially Unsafe Code - fopen**

Line: 2652 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

if (($v\_file\_compressed = @fopen($v\_gzip\_temp\_name, "rb")) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2652 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (($v\_file\_compressed = @fopen($v\_gzip\_temp\_name, "rb")) == 0) {

**STANDARD: Potentially Unsafe Code - fopen**

Line: 2684 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

if (($v\_file\_compressed = @fopen($v\_gzip\_temp\_name, "rb")) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2684 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (($v\_file\_compressed = @fopen($v\_gzip\_temp\_name, "rb")) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2696 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($this->zip\_fd, $v\_buffer, $v\_read\_size);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 2930 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

if (($this->zip\_fd = @fopen($this->zipname, 'rb')) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2930 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (($this->zip\_fd = @fopen($this->zipname, 'rb')) == 0) {

**STANDARD: Potentially Unsafe Code - fopen**

Line: 3478 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

if (($v\_dest\_file = @fopen($p\_entry['filename'], 'wb')) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 3478 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (($v\_dest\_file = @fopen($p\_entry['filename'], 'wb')) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 3495 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($v\_dest\_file, $v\_buffer, $v\_read\_size);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 3535 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

if (($v\_dest\_file = @fopen($p\_entry['filename'], 'wb')) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 3535 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (($v\_dest\_file = @fopen($p\_entry['filename'], 'wb')) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 3543 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($v\_dest\_file, $v\_file\_content, $p\_entry['size']);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 3600 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

if (($v\_dest\_file = @fopen($v\_gzip\_temp\_name, "wb")) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 3600 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (($v\_dest\_file = @fopen($v\_gzip\_temp\_name, "wb")) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 3608 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($v\_dest\_file, $v\_binary\_data, 10);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 3616 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($v\_dest\_file, $v\_buffer, $v\_read\_size);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 3622 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($v\_dest\_file, $v\_binary\_data, 8);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 3628 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

if (($v\_dest\_file = @fopen($p\_entry['filename'], 'wb')) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 3628 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (($v\_dest\_file = @fopen($p\_entry['filename'], 'wb')) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 3647 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($v\_dest\_file, $v\_buffer, $v\_read\_size);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 3722 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $v\_buffer;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 3733 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $v\_file\_content;

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 4224 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

Some bugs where found when a zip is encrypted/decrypted with 'crypt'.

**STANDARD: Potentially Unsafe Code - fopen**

Line: 4639 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

if (($v\_zip\_temp\_fd = @fopen($v\_zip\_temp\_name, 'wb')) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 4639 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (($v\_zip\_temp\_fd = @fopen($v\_zip\_temp\_name, 'wb')) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 4655 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($v\_zip\_temp\_fd, $v\_buffer, $v\_read\_size);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 4664 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($v\_zip\_temp\_fd, $v\_buffer, $v\_read\_size);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 4676 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($v\_zip\_temp\_fd, $v\_buffer, $v\_read\_size);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 4685 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($v\_zip\_temp\_fd, $v\_buffer, $v\_read\_size);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 4768 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

if (($v\_zip\_temp\_fd = @fopen($p\_archive\_filename, 'rb')) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 4768 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (($v\_zip\_temp\_fd = @fopen($p\_archive\_filename, 'rb')) == 0) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 4783 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($this->zip\_fd, $v\_buffer, $v\_read\_size);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 5062 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($p\_dest, $v\_buffer, $v\_read\_size);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 5069 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@fwrite($p\_dest, $v\_buffer, $v\_read\_size);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 5096 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\PCLZip\pclzip.lib.php

This function tries to do a simple rename() function. If it fails, it

**MEDIUM: Potentially Unsafe Code - md5**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Shared\trend\trendClass.php

MD5 Hashing algorithm.

$key = md5($trendType.$const.serialize($yValues).serialize($xValues));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 453 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\Alignment.php

MD5 Hashing algorithm.

return md5(

**MEDIUM: Potentially Unsafe Code - md5**

Line: 276 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\Border.php

MD5 Hashing algorithm.

return md5(

**MEDIUM: Potentially Unsafe Code - md5**

Line: 419 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\Borders.php

MD5 Hashing algorithm.

return md5(

**MEDIUM: Potentially Unsafe Code - md5**

Line: 438 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\Color.php

MD5 Hashing algorithm.

return md5(

**MEDIUM: Potentially Unsafe Code - md5**

Line: 270 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\Conditional.php

MD5 Hashing algorithm.

return md5(

**MEDIUM: Potentially Unsafe Code - md5**

Line: 314 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\Fill.php

MD5 Hashing algorithm.

return md5(

**MEDIUM: Potentially Unsafe Code - md5**

Line: 530 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\Font.php

MD5 Hashing algorithm.

return md5(

**MEDIUM: Potentially Unsafe Code - md5**

Line: 378 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\NumberFormat.php

MD5 Hashing algorithm.

return md5(

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 460 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\NumberFormat.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$format = preg\_replace('/^(\[\$[A-Z]\*-[0-9A-F]\*\])/i', '', $format);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 593 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\NumberFormat.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$format = preg\_replace('/(\\\(.))(?=(?:[^"]|"[^"]\*")\*$)/u', '"${2}"', $format);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 633 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\NumberFormat.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$format = preg\_replace('/\_./', ' ', $format);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 640 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\NumberFormat.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$format = preg\_replace($color\_regex, '', $format);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 663 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\NumberFormat.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$format = preg\_replace('/0,0/', '00', $format);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 664 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\NumberFormat.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$format = preg\_replace('/#,#/', '##', $format);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 676 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\NumberFormat.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$format = preg\_replace('/0,+/', '0', $format);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 677 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\NumberFormat.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$format = preg\_replace('/#,+/', '#', $format);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 693 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\NumberFormat.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$format = preg\_replace('/\\#/', '0', $format);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 696 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\NumberFormat.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$m = preg\_replace($n, '', $format);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 712 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\NumberFormat.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$value = preg\_replace($number\_regex, $value, $format);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 722 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\NumberFormat.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$value = preg\_replace($number\_regex, $value, $format);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 735 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\NumberFormat.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$value = preg\_replace('/\[\$([^\]]\*)\]/u', $currencyCode, $value);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 741 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\NumberFormat.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$format = preg\_replace("/\\\\/u", '\\', $format);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 198 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Style\Protection.php

MD5 Hashing algorithm.

return md5(

**MEDIUM: Potentially Unsafe Code - md5**

Line: 478 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Worksheet\BaseDrawing.php

MD5 Hashing algorithm.

return md5(

**MEDIUM: Potentially Unsafe Code - md5**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Worksheet\Drawing.php

MD5 Hashing algorithm.

return md5(

**MEDIUM: Potentially Unsafe Code - md5**

Line: 336 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Worksheet\HeaderFooterDrawing.php

MD5 Hashing algorithm.

return md5(

**MEDIUM: Potentially Unsafe Code - md5**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Worksheet\MemoryDrawing.php

MD5 Hashing algorithm.

$this->uniqueName = md5(rand(0, 9999). time() . rand(0, 9999));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Worksheet\MemoryDrawing.php

MD5 Hashing algorithm.

return md5(

**MEDIUM: Potentially Unsafe Code - md5**

Line: 270 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Worksheet\Drawing\Shadow.php

MD5 Hashing algorithm.

return md5(

**STANDARD: Potentially Unsafe Code - fopen**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\CSV.php

$fileHandle = fopen($pFilename, 'wb+');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\CSV.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fileHandle = fopen($pFilename, 'wb+');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\CSV.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($fileHandle, "\xEF\xBB\xBF");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\CSV.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($fileHandle, 'sep=' . $this->getDelimiter() . $this->lineEnding);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 347 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\CSV.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($pFileHandle, $line);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 347 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel2007.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$objZip->addFromString('xl/media/' . $image->getIndexedFilename(), file\_get\_contents($image->getPath()));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 367 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel2007.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$imageContents = file\_get\_contents($imagePath);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 414 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5.php

nothing to do if there are no drawings

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 476 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$blipData = file\_get\_contents($filename);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 480 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$blipData = file\_get\_contents($filename);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\HTML.php

$fileHandle = fopen($pFilename, 'wb+');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\HTML.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fileHandle = fopen($pFilename, 'wb+');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\HTML.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($fileHandle, $this->generateHTMLHeader(!$this->useInlineCss));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 169 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\HTML.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($fileHandle, $this->generateNavigation());

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\HTML.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($fileHandle, $this->generateSheetData());

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\HTML.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($fileHandle, $this->generateHTMLFooter());

**STANDARD: Potentially Unsafe Code - fopen**

Line: 640 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\HTML.php

if ($fp = fopen($filename, "rb", 0)) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 640 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\HTML.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if ($fp = fopen($filename, "rb", 0)) {

**STANDARD: Potentially Unsafe Code - fopen**

Line: 706 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\HTML.php

if ($fp = fopen($chartFileName, "rb", 0)) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 706 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\HTML.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if ($fp = fopen($chartFileName, "rb", 0)) {

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1264 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\HTML.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$cellData = preg\_replace("/(?m)(?:^|\\G) /", '&nbsp;', $cellData);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1582 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\HTML.php

TODO: Same for columns

**MEDIUM: Potentially Unsafe Code - md5**

Line: 531 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel2007\Drawing.php

MD5 Hashing algorithm.

preg\_match('{(\d+)}', md5($pReference), $m);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 275 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel2007\Style.php

and makes for a real WTF!

**MEDIUM: Potentially Unsafe Code - md5**

Line: 662 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel2007\Worksheet.php

MD5 Hashing algorithm.

$objWriter->writeAttribute('name', 'p' . md5($protectedCell));

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\BIFFwriter.php

\* I \_DO\_ maintain this code, and John McNamara has nothing to do with the

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\BIFFwriter.php

Give up. I'll fix this in a later version.

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 558 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Parser.php

TODO: use real error codes

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 633 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Parser.php

TODO: possible class value 0,1,2 check Formula.pm

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 638 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Parser.php

TODO: use real error codes

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 654 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Parser.php

TODO: use real error codes

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 726 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Parser.php

// TODO: use real error codes

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 805 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Parser.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ext\_ref = preg\_replace("/^'/", '', $ext\_ref);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 806 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Parser.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ext\_ref = preg\_replace("/'$/", '', $ext\_ref);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 850 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Parser.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ext\_ref = preg\_replace("/^'/", '', $ext\_ref);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 851 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Parser.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ext\_ref = preg\_replace("/'$/", '', $ext\_ref);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 879 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Parser.php

assume all references belong to this document

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 981 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Parser.php

FIXME: maximum possible value for Excel 5 (change this!!!)

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 983 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Parser.php

FIXME: this changes for BIFF8

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Workbook.php

\* I \_DO\_ maintain this code, and John McNamara has nothing to do with the

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 445 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Workbook.php

TODO: store external SUPBOOK records and XCT and CRN records

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 971 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Workbook.php

FIXME: only using internal SUPBOOK record

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

\* I \_DO\_ maintain this code, and John McNamara has nothing to do with the

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 505 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

@todo CFRule & CFHeader

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 580 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

public function printRowColHeaders($print = 1)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 582 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$this->\_print\_headers = $print;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1049 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url = preg\_replace('/^internal:/', '', $url);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url = preg\_replace('/^external:/', '', $url);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url = preg\_replace('/\

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$dir\_short = preg\_replace("/\.\.\\\/", '', $dir\_long) . "\0";

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1295 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

FIXME !!!

**MEDIUM: Potentially Unsafe Code - md5**

Line: 1624 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

MD5 Hashing algorithm.

$recordData .= PHPExcel\_Shared\_String::UTF8toBIFF8UnicodeLong('p' . md5($recordData));

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 2147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

Decide what to do by the type of break

**STANDARD: Potentially Unsafe Code - fopen**

Line: 2565 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

$bmp\_fd = @fopen($bitmap, "rb");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2565 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$bmp\_fd = @fopen($bitmap, "rb");

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 3678 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

@todo writeCFRule() => $blockLineStyle => Index Color for left line

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 3679 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

@todo writeCFRule() => $blockLineStyle => Index Color for right line

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 3680 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

@todo writeCFRule() => $blockLineStyle => Top-left to bottom-right on/off

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 3681 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

@todo writeCFRule() => $blockLineStyle => Bottom-left to top-right on/off

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 3683 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

@todo writeCFRule() => $blockColor => Index Color for top line

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 3684 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

@todo writeCFRule() => $blockColor => Index Color for bottom line

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 3685 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Worksheet.php

@todo writeCFRule() => $blockColor => Index Color for diagonal line

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\Excel5\Xf.php

\* I \_DO\_ maintain this code, and John McNamara has nothing to do with the

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\OpenDocument\Cell\Comment.php

TODO: Not realized in PHPExcel\_Comment yet.

**STANDARD: Potentially Unsafe Code - fopen**

Line: 329 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\PDF\Core.php

$fileHandle = fopen($pFilename, 'w');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 329 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\PDF\Core.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fileHandle = fopen($pFilename, 'w');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\PDF\DomPDF.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($fileHandle, $pdf->output());

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\PDF\mPDF.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($fileHandle, $pdf->Output('', 'S'));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\lib\PHPExcel\Writer\PDF\tcPDF.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($fileHandle, $pdf->output($pFilename, 'S'));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\content.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace($src, $dst, $str);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\content.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include($skin\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\content.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<p>'.str\_replace(G5\_PATH.'/', '', $skin\_file).'이 존재하지 않습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo latest('basic', $row['bo\_table'], 5, 70);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="hd\_h1"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_URL ?>"><img src="<?php echo G5\_IMG\_URL ?>/m\_logo.png" alt="<?php echo $config['cf\_title']; ?>"></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $row['me\_link']; ?>" target="\_<?php echo $row['me\_target']; ?>" class="gnb\_1da"><?php echo $row['me\_name'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="gnb\_2dli"><a href="<?php echo $row2['me\_link']; ?>" target="\_<?php echo $row2['me\_target']; ?>" class="gnb\_2da"><span></span><?php echo $row2['me\_name'] ?></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li id="gnb\_empty">메뉴 준비 중입니다.<?php if ($is\_admin) { ?> <br><a href="<?php echo G5\_ADMIN\_URL; ?>/menu\_list.php">관리자모드 &gt; 환경설정 &gt; 메뉴설정</a>에서 설정하세요.<?php } ?></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 id="container\_title" class="top" title="<?php echo get\_text($g5['title']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 189 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:history.back();"><i class="fa fa-chevron-left" aria-hidden="true"></i><span class="sound\_only">뒤로가기</span></a> <?php echo get\_head\_title($g5['title']); ?>

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\index.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

from `{$g5['board\_table']}` a left join `{$g5['group\_table']}` b on (a.gr\_id=b.gr\_id)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo latest('basic', $row['bo\_table'], 12, 25);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\newwin.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="hd\_pops\_<?php echo $nw['nw\_id'] ?>" class="hd\_pops" style="top:<?php echo $nw['nw\_top']?>px;left:<?php echo $nw['nw\_left']?>px;">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\newwin.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="hd\_pops\_con" style="width:<?php echo $nw['nw\_width'] ?>px;height:<?php echo $nw['nw\_height'] ?>px">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\newwin.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($nw['nw\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\newwin.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button class="hd\_pops\_reject hd\_pops\_<?php echo $nw['nw\_id']; ?> <?php echo $nw['nw\_disable\_hours']; ?>"><strong><?php echo $nw['nw\_disable\_hours']; ?></strong>시간 동안 다시 열람하지 않습니다.</button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\newwin.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button class="hd\_pops\_close hd\_pops\_<?php echo $nw['nw\_id']; ?>">닫기</button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\newwin.inc.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<span class="sound\_only">팝업레이어 알림이 없습니다.</span>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $config['cf\_analytics'];

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($theme\_cart\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="frmcartlist" id="sod\_bsk\_list" class="2017\_renewal\_itemform" method="post" action="<?php echo $cart\_action\_url; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[<?php echo $i; ?>]" value="<?php echo $row['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_name[<?php echo $i; ?>]" value="<?php echo get\_text($row['it\_name']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="ct\_chk[<?php echo $i; ?>]" value="1" id="ct\_chk\_<?php echo $i; ?>" class="selec\_chk" checked>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ct\_chk\_<?php echo $i; ?>"><span></span><b class="sound\_only">상품선택</b></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="li\_name"><?php echo $it\_name; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="total\_img"><?php echo $image; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="li\_mod"><?php echo $mod\_options; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sod\_opt"><?php echo $it\_options; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="prqty\_price li\_prqty\_sp"><span>판매가 </span><?php echo number\_format($row['ct\_price']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="prqty\_qty li\_prqty\_sp"><span>수량 </span><?php echo number\_format($sum['qty']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="prqty\_sc li\_prqty\_sp"><span>배송비 </span><?php echo $ct\_send\_cost; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="total\_point li\_prqty\_sp"><span>적립포인트 </span><strong><?php echo number\_format($sum['point']); ?></strong></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="total\_price total\_span"><span>소계 </span><strong><?php echo number\_format($sell\_price); ?></strong>원</div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sod\_bsk\_dvr"><strong><?php echo number\_format($send\_cost); ?> 원</strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 169 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><strong><?php echo number\_format($tot\_point); ?> 점</strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sod\_bsk\_cnt"><strong><?php echo number\_format($tot\_price); ?></strong> 원</dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="total">총계 <strong class="total\_cnt"><?php echo number\_format($tot\_price); ?>원</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 181 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="records" value="<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 186 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="naverpay-cart"><?php echo $naverpay\_request\_js.$naverpay\_button\_js; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $mshop\_ca\_row1['url']; ?>"><?php echo get\_text($mshop\_ca\_row1['ca\_name']); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<button class="sub\_ct\_toggle ct\_op">'.get\_text($mshop\_ca\_row1['ca\_name']).' 하위분류 열기</button>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $mshop\_ca\_row2['url']; ?>"><?php echo get\_text($mshop\_ca\_row2['ca\_name']); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<button type="button" class="sub\_ct\_toggle ct\_op">'.get\_text($mshop\_ca\_row2['ca\_name']).' 하위분류 열기</button>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $mshop\_ca\_row3['url']; ?>"><?php echo get\_text($mshop\_ca\_row3['ca\_name']); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<button type="button" class="sub\_ct\_toggle ct\_op">'.get\_text($mshop\_ca\_row3['ca\_name']).' 하위분류 열기</button>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $mshop\_ca\_href.$mshop\_ca\_row4['ca\_id']; ?>"><?php echo get\_text($mshop\_ca\_row4['ca\_name']); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<button type="button" class="sub\_ct\_toggle ct\_op">'.get\_text($mshop\_ca\_row4['ca\_name']).' 하위분류 열기</button>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $mshop\_ca\_href.$mshop\_ca\_row5['ca\_id']; ?>"><?php echo get\_text($mshop\_ca\_row5['ca\_name']); ?></a>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\coupon.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($theme\_coupon\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\coupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\coupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="cou\_tit"><?php echo $row['cp\_subject']; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\coupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="cou\_pri"><?php echo $cp\_price; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\coupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="cou\_target"><?php echo $cp\_target; ?> <i class="fa fa-angle-right" aria-hidden="true"></i></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\coupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="cou\_date"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo substr($row['cp\_start'], 2, 8); ?> ~ <i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo substr($row['cp\_end'], 2, 8); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\event.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="sev\_admin"><a href="'.G5\_ADMIN\_URL.'/shop\_admin/itemeventform.php?w=u&amp;ev\_id='.$ev['ev\_id'].'" class="btn\_admin">이벤트 관리</a></div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\event.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="sev\_hhtml">'.conv\_content($ev['ev\_head\_html'], 1).'</div>';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\event.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$skin = preg\_replace('#\.+(\/|\\\)#', '', $skin);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\event.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\event.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div align="center">'.$ev['ev\_mobile\_skin'].' 파일을 찾을 수 없습니다.<br>관리자에게 알려주시면 감사하겠습니다.</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\event.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_paging($config['cf\_mobile\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page=");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\event.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="sev\_thtml">'.conv\_content($ev['ev\_tail\_html'], 1).'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**HIGH: Potentially Unsafe Code - User Controlled Variable Used on System Command Line**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\item.php

The application appears to allow the use of a user-controlled variable within backticks, allowing commandline execution.

$sql = " select count(\*) as cnt from `{$g5['g5\_shop\_item\_use\_table']}` where it\_id = '{$it\_id}' and is\_confirm = '1' ";

**HIGH: Potentially Unsafe Code - User Controlled Variable Used on System Command Line**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\item.php

The application appears to allow the use of a user-controlled variable within backticks, allowing commandline execution.

$sql = " select count(\*) as cnt from `{$g5['g5\_shop\_item\_qa\_table']}` where it\_id = '{$it\_id}' ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 200 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="sit\_hhtml">'.conv\_content($it['it\_mobile\_head\_html'], 1).'</div>';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 218 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\item.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($skin\_dir.'/item.form.skin.php');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 225 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo conv\_content($it['it\_mobile\_tail\_html'], 1);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 5 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\iteminfo.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$info = isset($\_GET['info']) ? preg\_replace('/[^0-9a-z]/i', '', $\_GET['info']) : '';

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\iteminfo.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " select count(\*) as cnt from `{$g5['g5\_shop\_item\_use\_table']}` where it\_id = '{$it\_id}' and is\_confirm = '1' ";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\iteminfo.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = " select count(\*) as cnt from `{$g5['g5\_shop\_item\_qa\_table']}` where it\_id = '{$it\_id}' ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\iteminfo.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $href; ?>" <?php if ($info == '') echo 'class="sanchor\_on"'; ?>>DETAIL</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\iteminfo.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($default['de\_baesong\_content']) { ?><li><a href="<?php echo $href; ?>&amp;info=dvr" <?php if ($info == 'dvr') echo 'class="sanchor\_on"'; ?>>INFO</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\iteminfo.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $href; ?>&amp;info=use" <?php if ($info == 'use') echo 'class="sanchor\_on"'; ?>>REVIEW<span class="item\_use\_count"><?php echo $item\_use\_count; ?></span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\iteminfo.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $href; ?>&amp;info=qa" <?php if ($info == 'qa') echo 'class="sanchor\_on"'; ?>>Q&amp;A<span class="item\_qa\_count"><?php echo $item\_qa\_count; ?></span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\iteminfo.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo pg\_anchor($info); ?>

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemqa.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql\_common = " from `{$g5['g5\_shop\_item\_qa\_table']}` where it\_id = '{$it\_id}' ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemqa.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo str\_replace(G5\_PATH.'/', '', $itemqa\_skin).' 스킨 파일이 존재하지 않습니다.';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemqa.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($itemqa\_skin);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemqaform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$w = isset($\_REQUEST['w']) ? preg\_replace('/[^0-9a-z]/i', '', trim($\_REQUEST['w'])) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemqaform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$iq\_id = isset($\_REQUEST['iq\_id']) ? preg\_replace('/[^0-9]/', '', trim($\_REQUEST['iq\_id'])) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo str\_replace(G5\_PATH.'/', '', $itemqaform\_skin).' 스킨 파일이 존재하지 않습니다.';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemqaform.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($itemqaform\_skin);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemqalist.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql\_common = " from `{$g5['g5\_shop\_item\_qa\_table']}` a join `{$g5['g5\_shop\_item\_table']}` b on (a.it\_id=b.it\_id) ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo str\_replace(G5\_PATH.'/', '', $itemqalist\_skin).' 스킨 파일이 존재하지 않습니다.';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemqalist.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($itemqalist\_skin);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemrecommend.php

MD5 Hashing algorithm.

$token = md5(uniqid(rand(), true));

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemrecommend.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title']; ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemrecommend.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo $token; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemrecommend.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id" value="<?php echo $it\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemuse.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql\_common = " from `{$g5['g5\_shop\_item\_use\_table']}` where it\_id = '{$it\_id}' and is\_confirm = '1' ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemuse.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo str\_replace(G5\_PATH.'/', '', $itemuse\_skin).' 스킨 파일이 존재하지 않습니다.';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemuse.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($itemuse\_skin);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemuseform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$w = isset($\_REQUEST['w']) ? preg\_replace('/[^0-9a-z]/i', '', trim($\_REQUEST['w'])) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemuseform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$is\_id = $\_REQUEST['is\_id'] ? preg\_replace('/[^0-9]/', '', trim($\_REQUEST['is\_id'])) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo str\_replace(G5\_PATH.'/', '', $itemuseform\_skin).' 스킨 파일이 존재하지 않습니다.';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemuseform.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($itemuseform\_skin);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemuselist.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql\_common = " from `{$g5['g5\_shop\_item\_use\_table']}` a join `{$g5['g5\_shop\_item\_table']}` b on (a.it\_id=b.it\_id) ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo str\_replace(G5\_PATH.'/', '', $itemuselist\_skin).' 스킨 파일이 존재하지 않습니다.';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\itemuselist.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($itemuselist\_skin);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 5 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\largeimage.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$no = isset($\_GET['no']) ? preg\_replace('/[^0-9a-z]/i', '', $\_GET['no']) : '';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\largeimage.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($skin);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\largeimage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<p>'.str\_replace(G5\_PATH.'/', '', $skin).'파일이 존재하지 않습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="sct\_hhtml">'.conv\_content($ca['ca\_mobile\_head\_html'], 1).'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="sct\_nofile">'.str\_replace(G5\_PATH.'/', '', $skin\_file).' 파일을 찾을 수 없습니다.<br>관리자에게 알려주시면 감사하겠습니다.</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" id="btn\_more\_item" data-url="<?php echo $ajax\_url; ?>" data-page="<?php echo $page; ?>">더보기 +</button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 186 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="sct\_thtml">'.conv\_content($ca['ca\_mobile\_tail\_html'], 1).'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 193 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "\n<!-- {$ca['ca\_mobile\_skin']} -->\n";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 4 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\listtype.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$type = isset($\_REQUEST['type']) ? preg\_replace("/[\<\>\'\"\\\'\\\"\%\=\(\)\s]/", "", $\_REQUEST['type']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\listtype.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$skin = preg\_replace('#\.+[\\\/]#', '', $skin);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\listtype.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\listtype.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div align="center">'.$skin.' 파일을 찾을 수 없습니다.<br>관리자에게 알려주시면 감사하겠습니다.</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\listtype.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_paging($config['cf\_mobile\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page=");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\mypage.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($theme\_mypage\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($member['mb\_id']); ?> <strong><?php echo $member['mb\_id'] ? $member['mb\_name'] : '비회원'; ?></strong>님

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == 'super') { ?><li><a href="<?php echo G5\_ADMIN\_URL; ?>/" class="btn\_admin">관리자</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_SHOP\_URL; ?>/coupon.php" target="\_blank" class="win\_coupon"><?php echo number\_format($cp\_count); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_BBS\_URL; ?>/point.php" target="\_blank" class="win\_point"><?php echo number\_format($member['mb\_point']); ?>점</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo ($member['mb\_tel'] ? $member['mb\_tel'] : '미등록'); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo ($member['mb\_email'] ? $member['mb\_email'] : '미등록'); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $member['mb\_today\_login']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $member['mb\_datetime']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo sprintf("(%s%s)", $member['mb\_zip1'], $member['mb\_zip2']).' '.print\_address($member['mb\_addr1'], $member['mb\_addr2'], $member['mb\_addr3'], $member['mb\_addr\_jibeon']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="wish\_img"><?php echo $image; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_shop\_item($row['it\_id'], true); ?>" class="info\_link"><?php echo stripslashes($row['it\_name']); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="info\_date"><?php echo substr($row['wi\_time'], 2, 8); ?></span>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderaddress.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($theme\_orderaddress\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="forderaddress" method="post" action="<?php echo $order\_action\_url; ?>" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ad\_id[<?php echo $i; ?>]" value="<?php echo $row['ad\_id'];?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk[]" value="<?php echo $i;?>" id="chk\_<?php echo $i;?>" class="ad\_chk selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i;?>"><span></span><strong class="sound\_only">배송지선택</strong></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ad\_subject<?php echo $i;?>" class="sound\_only">배송지명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ad\_subject[<?php echo $i; ?>]" value="<?php echo $row['ad\_subject']; ?>" class="ad\_subject" maxlength="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="addr\_name"><?php echo get\_text($row['ad\_name']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="addr\_addr"><?php echo print\_address($row['ad\_addr1'], $row['ad\_addr2'], $row['ad\_addr3'], $row['ad\_jibeon']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="addr\_tel"><i class="fa fa-phone" aria-hidden="true"></i> <?php echo $row['ad\_tel']; ?> / <i class="fa fa-mobile" aria-hidden="true"></i> <?php echo $row['ad\_hp']; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" value="<?php echo $addr; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>?w=d&amp;ad\_id=<?php echo $row['ad\_id']; ?>" id="btn\_del" class="del\_address">삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="ad\_default" value="<?php echo $row['ad\_id'];?>" id="ad\_default<?php echo $i;?>" <?php if($row['ad\_default']) echo 'checked="checked"';?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ad\_default<?php echo $i;?>" class="add\_lb">기본배송지</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($config['cf\_mobile\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$goods = preg\_replace("/\?|\'|\"|\||\,|\&|\;/", "", $row['it\_name']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[<?php echo $i; ?>]" value="<?php echo $row['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 174 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_name[<?php echo $i; ?>]" value="<?php echo get\_text($row['it\_name']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 175 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_price[<?php echo $i; ?>]" value="<?php echo $sell\_price; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_notax[<?php echo $i; ?>]" value="<?php echo $row['it\_notax']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cp\_id[<?php echo $i; ?>]" value="">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cp\_price[<?php echo $i; ?>]" value="0">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 182 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $it\_name; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 185 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="total\_img"><?php echo $image; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 186 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sod\_opt"><?php echo $it\_options; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="li\_mod" ><?php echo $cp\_button; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 191 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="prqty\_price li\_prqty\_sp"><span>판매가 </span><?php echo number\_format($row['ct\_price']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 192 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="prqty\_qty li\_prqty\_sp"><span>수량 </span><?php echo number\_format($sum['qty']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 193 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="prqty\_sc li\_prqty\_sp"><span>배송비 </span><?php echo $ct\_send\_cost; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 194 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="total\_point li\_prqty\_sp"><span>적립포인트 </span><strong><?php echo number\_format($sum['point']); ?></strong></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 197 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="total\_price total\_span"><span>주문금액 </span><strong><?php echo number\_format($sell\_price); ?></strong></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 229 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sod\_bsk\_sell"><strong><?php echo number\_format($tot\_sell\_price); ?> 원</strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 235 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sod\_bsk\_dvr"><strong><?php echo number\_format($send\_cost); ?> 원</strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 238 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sod\_bsk\_point"><strong><?php echo number\_format($tot\_point); ?> 점</strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 242 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong id="ct\_tot\_price"><?php echo number\_format($tot\_price); ?></strong> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 273 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="forderform" method="post" action="<?php echo $order\_action\_url; ?>" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 274 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_price" value="<?php echo $tot\_sell\_price; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 275 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="org\_od\_price" value="<?php echo $tot\_sell\_price; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 276 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_send\_cost" value="<?php echo $send\_cost; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 282 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $content; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 291 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_name" value="<?php echo isset($member['mb\_name']) ? get\_text($member['mb\_name']) : ''; ?>" id="od\_name" required class="frm\_input required" maxlength="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 306 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_tel" value="<?php echo get\_text($member['mb\_tel']); ?>" id="od\_tel" required class="frm\_input required" maxlength="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 310 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_hp" value="<?php echo get\_text($member['mb\_hp']); ?>" id="od\_hp" class="frm\_input" maxlength="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 316 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_zip" value="<?php echo $member['mb\_zip1'].$member['mb\_zip2']; ?>" id="od\_zip" required class="frm\_input required" size="5" maxlength="6">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 319 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_addr1" value="<?php echo get\_text($member['mb\_addr1']) ?>" id="od\_addr1" required class="frm\_input frm\_address required">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 321 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_addr2" value="<?php echo get\_text($member['mb\_addr2']) ?>" id="od\_addr2" class="frm\_input frm\_address">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 323 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_addr3" value="<?php echo get\_text($member['mb\_addr3']) ?>" id="od\_addr3" class="frm\_input frm\_address" readonly="readonly">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 324 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_addr\_jibeon" value="<?php echo get\_text($member['mb\_addr\_jibeon']); ?>"><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 329 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="email" name="od\_email" value="<?php echo $member['mb\_email']; ?>" id="od\_email" required class="frm\_input required" maxlength="100">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 340 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<option value="'.$sdate.'">'.$sdate.' ('.get\_yoil($sdate).')</option>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 405 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div><?php echo $addr\_list; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 530 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><span id="od\_tot\_price"><?php echo number\_format($tot\_price); ?></span>원</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 559 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><input type="radio" id="od\_settle\_kakaopay" name="od\_settle\_case" value="KAKAOPAY" '.$checked.'> <label for="od\_settle\_kakaopay" class="kakaopay\_icon lb\_icon">KAKAOPAY</label></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 566 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><input type="radio" id="od\_settle\_bank" name="od\_settle\_case" value="무통장" '.$checked.'> <label for="od\_settle\_bank" class="lb\_icon bank\_icon">무통장입금</label></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 573 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><input type="radio" id="od\_settle\_vbank" name="od\_settle\_case" value="가상계좌" '.$checked.'> <label for="od\_settle\_vbank" class="lb\_icon vbank\_icon">'.$escrow\_title.'가상계좌</label></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 580 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><input type="radio" id="od\_settle\_iche" name="od\_settle\_case" value="계좌이체" '.$checked.'> <label for="od\_settle\_iche" class="lb\_icon iche\_icon">'.$escrow\_title.'계좌이체</label></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 587 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><input type="radio" id="od\_settle\_hp" name="od\_settle\_case" value="휴대폰" '.$checked.'> <label for="od\_settle\_hp" class="lb\_icon hp\_icon">휴대폰</label></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 594 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><input type="radio" id="od\_settle\_card" name="od\_settle\_case" value="신용카드" '.$checked.'> <label for="od\_settle\_card" class="lb\_icon card\_icon">신용카드</label></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 638 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo run\_replace('shop\_orderform\_easypay\_buttons', implode(PHP\_EOL, $easypay\_prints), $easypay\_prints, $multi\_settle);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 643 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><input type="radio" id="od\_settle\_samsungpay" data-case="samsungpay" name="od\_settle\_case" value="삼성페이" '.$checked.'> <label for="od\_settle\_samsungpay" class="samsung\_pay lb\_icon">삼성페이</label></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 649 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><input type="radio" id="od\_settle\_inicislpay" data-case="lpay" name="od\_settle\_case" value="lpay" '.$checked.'> <label for="od\_settle\_inicislpay" class="inicis\_lpay">L.pay</label></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 655 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><input type="radio" id="od\_settle\_inicis\_kakaopay" data-case="inicis\_kakaopay" name="od\_settle\_case" value="inicis\_kakaopay" '.$checked.'> <label for="od\_settle\_inicis\_kakaopay" title="KG 이니시스 카카오페이" class="inicis\_kakaopay">KG 이니시스 카카오페이</label></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 680 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div><input type="hidden" name="max\_temp\_point" value="'.$temp\_point.'"><label for="od\_temp\_point">사용 포인트('.$point\_unit.'점 단위)</label> <input type="text" id="od\_temp\_point" name="od\_temp\_point" value="0" size="10"> 점</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 681 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="sod\_frm\_pt\_info"><span><strong>보유포인트</strong>'.display\_point($member['mb\_point']).'</span><span class="max\_point\_box"><strong>최대사용가능포인트</strong><em id="use\_max\_point">'.display\_point($temp\_point).'</em></span></div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 708 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $bank\_account;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 789 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

{ it\_id: it\_id, sw\_direct: "<?php echo $sw\_direct; ?>" },

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var mb\_point = parseInt(<?php echo $member['mb\_point']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var max\_point = parseInt(<?php echo $default['de\_settle\_max\_point']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var point\_unit = parseInt(<?php echo $default['de\_settle\_point\_unit']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1407 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

f.P\_RETURN\_URL.value = "<?php echo $return\_url.$od\_id; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1551 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var point\_unit = parseInt(<?php echo $default['de\_settle\_point\_unit']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1566 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (temp\_point > <?php echo (int)$member['mb\_point']; ?>) {

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1640 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$("#od\_hope\_date").datepicker({ changeMonth: true, changeYear: true, dateFormat: "yy-mm-dd", showButtonPanel: true, yearRange: "c-99:c+99", minDate: "+<?php echo (int)$default['de\_hope\_date\_after']; ?>d;", maxDate: "+<?php echo (int)$default['de\_hope\_date\_after'] + 6; ?>d;" });

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderformupdate.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = "ALTER TABLE `{$g5['g5\_shop\_order\_table']}`

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 285 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_b\_zip = preg\_replace('/[^0-9]/', '', $od\_b\_zip);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 367 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 418 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 444 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 470 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 486 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 501 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 578 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_zip = preg\_replace('/[^0-9]/', '', $od\_zip);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 826 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$recv\_number = preg\_replace("/[^0-9]/", "", $recv\_numbers[$s]);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 827 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace("/[^0-9]/", "", $send\_numbers[$s]);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 849 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$recv\_number = preg\_replace("/[^0-9]/", "", $od\_hp);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 850 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace("/[^0-9]/", "", $default['de\_admin\_company\_tel']);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 909 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderformupdate.php

MD5 Hashing algorithm.

$uid = md5($od\_id.G5\_TIME\_YMDHIS.$REMOTE\_ADDR);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiry.php

MD5 Hashing algorithm.

$uid = md5($row['od\_id'].$row['od\_time'].$row['od\_ip']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiry.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($config['cf\_mobile\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiry.sub.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($theme\_inquiry\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiry.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (!$limit) { ?>총 <?php echo $cnt; ?> 건<?php } ?>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiry.sub.php

MD5 Hashing algorithm.

$uid = md5($row['od\_id'].$row['od\_time'].$row['od\_ip']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiry.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_SHOP\_URL; ?>/orderinquiryview.php?od\_id=<?php echo $row['od\_id']; ?>&amp;uid=<?php echo $uid; ?>" class="idtime\_link"><?php echo $row['od\_id']; ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiry.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="idtime\_time"><?php echo substr($row['od\_time'],2,25); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiry.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $ct\_name; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiry.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo display\_price($row['od\_receipt\_price']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiry.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="inv\_status"><?php echo $od\_status; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiry.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $od\_invoice; ?>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($theme\_inquiryview\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sod\_fin\_no">주문번호 <strong><?php echo $od\_id; ?></strong></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo shop\_item\_url($row['it\_id']); ?>"><strong><?php echo $row['it\_name']; ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo shop\_item\_url($row['it\_id']); ?>" class="total\_img"><?php echo $image; ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="prqty\_stat"><span class="sound\_only">상태</span><?php echo $opt['ct\_status']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sod\_opt"><span class="opt\_name"><?php echo get\_text($opt['ct\_option']); ?></span></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="prqty\_price li\_prqty\_sp"><span>판매가 </span><?php echo number\_format($opt\_price); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="prqty\_qty li\_prqty\_sp"><span>수량 </span><?php echo number\_format($opt['ct\_qty']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="prqty\_sc li\_prqty\_sp"><span>배송비 </span><?php echo $ct\_send\_cost; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="total\_point li\_prqty\_sp"><span>적립포인트 </span><?php echo number\_format($point); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="total\_price total\_span"><span>주문금액 </span><?php echo number\_format($sell\_price); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sod\_bsk\_dvr"><strong><?php echo number\_format($od['od\_cart\_price']); ?> 원</strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 174 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sod\_bsk\_dvr"><strong><?php echo number\_format($od['od\_cart\_coupon']); ?> 원</strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sod\_bsk\_dvr"><strong><?php echo number\_format($od['od\_coupon']); ?> 원</strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 184 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sod\_bsk\_dvr"><strong><?php echo number\_format($od['od\_send\_cost']); ?> 원</strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 189 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sod\_bsk\_dvr"><strong><?php echo number\_format($od['od\_send\_coupon']); ?> 원</strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 194 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sod\_bsk\_dvr"><strong><?php echo number\_format($od['od\_send\_cost2']); ?> 원</strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 199 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sod\_bsk\_dvr"><strong><?php echo number\_format($od['od\_cancel\_price']); ?> 원</strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 203 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sod\_bsk\_point"><strong><?php echo number\_format($tot\_point); ?> 점</strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 206 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sod\_bsk\_cnt"><strong><?php echo number\_format($tot\_price); ?> 원</strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 272 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od\_id; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 276 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od['od\_time']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 280 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo check\_pay\_name\_replace($od['od\_settle\_case'], $od, 1); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 284 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od\_receipt\_price; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 292 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od['od\_receipt\_time']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 302 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><?php echo $app\_no\_subj; ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 303 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $app\_no; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 314 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_deposit\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 318 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_bank\_account']); ?></td>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 335 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

MD5 Hashing algorithm.

$LGD\_HASHDATA = md5($LGD\_MID.$LGD\_TID.$LGD\_MERTKEY);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 344 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $hp\_receipt\_script; ?>">영수증 출력</a>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 354 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

MD5 Hashing algorithm.

$LGD\_HASHDATA = md5($LGD\_MID.$LGD\_TID.$LGD\_MERTKEY);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 363 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $card\_receipt\_script; ?>">영수증 출력</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 372 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $card\_receipt\_script; ?>">영수증 출력</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 386 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_point($od['od\_receipt\_point']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 397 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_price($od['od\_refund\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 438 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $cash\_receipt\_script; ?>">현금영수증 확인하기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 444 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="window.open('<?php echo G5\_SHOP\_URL; ?>/taxsave.php?od\_id=<?php echo $od\_id; ?>', 'taxsave', 'width=550,height=400,scrollbars=1,menus=0');">현금영수증을 발급하시려면 클릭하십시오.</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 466 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 470 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_tel']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 474 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_hp']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 478 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text(sprintf("(%s%s)", $od['od\_zip1'], $od['od\_zip2']).' '.print\_address($od['od\_addr1'], $od['od\_addr2'], $od['od\_addr3'], $od['od\_addr\_jibeon'])); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 482 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_email']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 499 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_b\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 503 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_b\_tel']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 507 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_b\_hp']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 511 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text(sprintf("(%s%s)", $od['od\_b\_zip1'], $od['od\_b\_zip2']).' '.print\_address($od['od\_b\_addr1'], $od['od\_b\_addr2'], $od['od\_b\_addr3'], $od['od\_b\_addr\_jibeon'])); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 520 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo substr($od['od\_hope\_date'],0,10).' ('.get\_yoil($od['od\_hope\_date']).')' ;?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 528 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo conv\_content($od['od\_memo'], 0); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 549 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od['od\_delivery\_company']; ?> <?php echo get\_delivery\_inquiry($od['od\_delivery\_company'], $od['od\_invoice'], 'dvr\_link'); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 553 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od['od\_invoice']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 557 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od['od\_invoice\_time']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 582 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo display\_price($tot\_price); ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 588 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<strong>'.display\_price($misu\_price).'</strong>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 594 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $wanbul; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 597 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><span class="title"><i class="fa fa-angle-right" aria-hidden="true"></i> 포인트 결제</span><?php echo number\_format($od['od\_receipt\_point']); ?> 점</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 598 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><span class="title"><i class="fa fa-angle-right" aria-hidden="true"></i> 실결제</span><?php echo number\_format($od['od\_receipt\_price']); ?> 원</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 616 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_id" value="<?php echo $od['od\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 617 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo $token; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 646 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="e\_trade\_no" value="<?php echo $od['od\_tno']; ?>"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 650 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="deposit\_no" value="<?php echo $deposit\_no; ?>"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 654 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="req\_name" value="<?php echo $od['od\_deposit\_name']; ?>"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpay.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_paging($config['cf\_mobile\_pages'], $page, $total\_page, $\_SERVER['SCRIPT\_NAME'].'?'.$qstr.'&amp;page=');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="forderform" method="post" action="<?php echo $order\_action\_url; ?>" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="pp\_id" value="<?php echo $pp['pp\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo conv\_content($pp['pp\_content'], 0); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_price($pp['pp\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="pp\_name" value="<?php echo get\_text($pp['pp\_name']); ?>" id="pp\_name" required class="required frm\_input"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="email" name="pp\_email" value="<?php echo $member['mb\_email']; ?>" id="pp\_email" required class="required frm\_input"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="pp\_hp" value="<?php echo get\_text($member['mb\_hp']); ?>" id="pp\_hp" class="frm\_input"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><input type="radio" id="pp\_settle\_vbank" name="pp\_settle\_case" value="가상계좌" '.$checked.'> <label for="pp\_settle\_vbank"><span></span>'.$escrow\_title.'가상계좌</label></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><input type="radio" id="pp\_settle\_iche" name="pp\_settle\_case" value="계좌이체" '.$checked.'> <label for="pp\_settle\_iche"><span></span>'.$escrow\_title.'계좌이체</label></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><input type="radio" id="pp\_settle\_hp" name="pp\_settle\_case" value="휴대폰" '.$checked.'> <label for="pp\_settle\_hp"><span></span>휴대폰</label></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><input type="radio" id="pp\_settle\_card" name="pp\_settle\_case" value="신용카드" '.$checked.'> <label for="pp\_settle\_card"><span></span>신용카드</label></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 207 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

f.P\_RETURN\_URL.value = "<?php echo $return\_url.$pp\_id; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 287 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var tot\_price = <?php echo (int)$pp['pp\_price']; ?>;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$pp\_id = isset($\_POST['pp\_id']) ? preg\_replace('/[^0-9]/', '', $\_POST['pp\_id']) : 0;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$good\_mny = isset($\_POST['good\_mny']) ? preg\_replace('/[^0-9]/', '', $\_POST['good\_mny']) : 0;

**MEDIUM: Potentially Unsafe Code - md5**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayformupdate.php

MD5 Hashing algorithm.

$hash\_data = md5($pp\_id.$good\_mny.$pp['pp\_time']);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayformupdate.php

MD5 Hashing algorithm.

$uid = md5($pp['pp\_id'].$pp['pp\_time'].$\_SERVER['REMOTE\_ADDR']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$pp\_receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$pp\_receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$pp\_receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 260 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayformupdate.php

MD5 Hashing algorithm.

$uid = md5($pp['pp\_id'].$pp['pp\_time'].$\_SERVER['REMOTE\_ADDR']);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

MD5 Hashing algorithm.

if (! (isset($pp['pp\_id']) && $pp['pp\_id']) || (md5($pp['pp\_id'].$pp['pp\_time'].$\_SERVER['REMOTE\_ADDR']) != get\_session('ss\_personalpay\_uid'))) {

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p id="sod\_fin\_no">개인결제번호 <strong><?php echo $pp\_id; ?></strong></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $pp['od\_id']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $pp['pp\_settle\_case']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $pp\_receipt\_price; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo is\_null\_time($pp['pp\_receipt\_time']) ? '' : $pp['pp\_receipt\_time']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><?php echo $app\_no\_subj; ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $app\_no; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($pp['pp\_deposit\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($pp['pp\_bank\_account']); ?></td>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

MD5 Hashing algorithm.

$LGD\_HASHDATA = md5($LGD\_MID.$LGD\_TID.$LGD\_MERTKEY);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $hp\_receipt\_script; ?>">영수증 출력</a>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

MD5 Hashing algorithm.

$LGD\_HASHDATA = md5($LGD\_MID.$LGD\_TID.$LGD\_MERTKEY);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $card\_receipt\_script; ?>">영수증 출력</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 230 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $cash\_receipt\_script; ?>">현금영수증 확인하기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="window.open('<?php echo G5\_SHOP\_URL; ?>/taxsave.php?tx=personalpay&od\_id=<?php echo $pp\_id; ?>', 'taxsave', 'width=550,height=400,scrollbars=1,menus=0');">현금영수증을 발급하시려면 클릭하십시오.</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 256 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo display\_price($pp['pp\_price']); ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 262 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<strong>'.display\_price($misu\_price).'</strong>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 268 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $wanbul; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 289 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="e\_trade\_no" value="<?php echo $pp['pp\_tno']; ?>"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 293 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="deposit\_no" value="<?php echo $deposit\_no; ?>"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 297 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="req\_name" value="<?php echo $pp['pp\_deposit\_name']; ?>"></td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\search.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$qcaid = isset($\_GET['qcaid']) ? preg\_replace('#[^a-z0-9]#i', '', trim($\_GET['qcaid'])) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\search.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$qfrom = isset($\_GET['qfrom']) ? preg\_replace('/[^0-9]/', '', trim($\_GET['qfrom'])) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\search.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$qto = isset($\_GET['qto']) ? preg\_replace('/[^0-9]/', '', trim($\_GET['qto'])) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\search.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$qsort = preg\_replace("/[\<\>\'\"\\\'\\\"\%\=\(\)\s]/", "", $qsort);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo str\_replace(G5\_PATH.'/', '', $search\_skin).' 스킨 파일이 존재하지 않습니다.';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\search.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($search\_skin);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ((!$bo\_table || $w == 's' ) && defined('\_INDEX\_')) { ?><h1><?php echo $config['cf\_title'] ?></h1><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="logo"><a href="<?php echo G5\_SHOP\_URL; ?>/"><img src="<?php echo G5\_DATA\_URL; ?>/common/mobile\_logo\_img" alt="<?php echo $config['cf\_title']; ?> 메인"></a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="q" value="<?php echo stripslashes(get\_text(get\_search\_string($q))); ?>" id="sch\_str" required class="frm\_input" placeholder="검색어를 입력해주세요">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="container" class="<?php echo implode(' ', $container\_class); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ((!$bo\_table || $w == 's' ) && !defined('\_INDEX\_')) { ?><h1 id="container\_title"><a href="javascript:history.back()" class="btn\_back"><i class="fa fa-chevron-left" aria-hidden="true"></i><span class="sound\_only">뒤로</span></a> <?php echo $g5['title'] ?></h1><?php }

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $config['cf\_title']; ?> 정보</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="ft\_logo"><a href="<?php echo G5\_SHOP\_URL; ?>/"><img src="<?php echo G5\_DATA\_URL; ?>/common/mobile\_logo\_img2" alt="<?php echo $config['cf\_title']; ?> 메인"></a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>회사명</b> <?php echo $default['de\_admin\_company\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>주소</b> <?php echo $default['de\_admin\_company\_addr']; ?></span><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>사업자 등록번호</b> <?php echo $default['de\_admin\_company\_saupja\_no']; ?></span><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>대표</b> <?php echo $default['de\_admin\_company\_owner']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>전화</b> <?php echo $default['de\_admin\_company\_tel']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>팩스</b> <?php echo $default['de\_admin\_company\_fax']; ?></span><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <span><b>운영자</b> <?php echo $admin['mb\_name']; ?></span><br> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>통신판매업신고번호</b> <?php echo $default['de\_admin\_tongsin\_no']; ?></span><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>개인정보 보호책임자</b> <?php echo $default['de\_admin\_info\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($default['de\_admin\_buga\_no']) echo '<span><b>부가통신사업신고번호</b> '.$default['de\_admin\_buga\_no'].'</span>'; ?><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

Copyright &copy; 2001-2013 <?php echo $default['de\_admin\_company\_name']; ?>. All Rights Reserved.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $config['cf\_analytics'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $config['cf\_analytics'];

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\wishlist.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($theme\_wishlist\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="wish\_img"><a href="<?php echo shop\_item\_url($row['it\_id']); ?>"><?php echo $image; ?></a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo shop\_item\_url($row['it\_id']); ?>" class="wish\_prd"><?php echo stripslashes($row['it\_name']); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="info\_price"><?php echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n"; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="info\_date"><?php echo substr($row['wi\_time'], 2, 17); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_it\_id[<?php echo $i; ?>]" value="1" id="chk\_it\_id\_<?php echo $i; ?>" onclick="out\_cd\_check(this, '<?php echo $out\_cd; ?>');" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_it\_id\_<?php echo $i; ?>"><span></span><b class="sound\_only"><?php echo $row['it\_name']; ?></b></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[<?php echo $i; ?>]" value="<?php echo $row['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_type[<?php echo $row['it\_id']; ?>][0]" value="0">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_id[<?php echo $row['it\_id']; ?>][0]" value="">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_value[<?php echo $row['it\_id']; ?>][0]" value="<?php echo $row['it\_name']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ct\_qty[<?php echo $row['it\_id']; ?>][0]" value="1">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="wish\_del"><a href="<?php echo G5\_SHOP\_URL; ?>/wishupdate.php?w=d&amp;wi\_id=<?php echo $row['wi\_id']; ?>"><i class="fa fa-trash" aria-hidden="true"></i><span class="sound\_only">삭제</span></a></span>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\\_common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sort = preg\_replace("/[\<\>\'\"\\\'\\\"\%\=\(\)\s]/", "", $sort);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_OID" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_GOODS" value="<?php echo $goods; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_AMT" value="<?php echo $tot\_price; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_MID" value="<?php echo $default['de\_inicis\_mid']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_NEXT\_URL" value="<?php echo $next\_url; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_NOTI\_URL" value="<?php echo $noti\_url; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_RESERVED" value="<?php echo get\_inicis\_app\_scheme(); ?>bank\_receipt=N&twotrs\_isp=Y&block\_isp=Y<?php echo $useescrow.$inicis\_cardpoint; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="DEF\_RESERVED" value="<?php echo get\_inicis\_app\_scheme(); ?>bank\_receipt=N&twotrs\_isp=Y&block\_isp=Y<?php echo $useescrow.$inicis\_cardpoint; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_NOTI" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_mny" value="<?php echo $tot\_price; ?>" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 5 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_mny" value="<?php echo $tot\_price ?>" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_tax\_mny" value="<?php echo $comm\_tax\_mny; ?>"> <!-- 과세금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_vat\_mny" value="<?php echo $comm\_vat\_mny; ?>"> <!-- 부가세 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_free\_mny" value="<?php echo $comm\_free\_mny; ?>"> <!-- 비과세 금액 -->

**MEDIUM: Potentially Unsafe Code - md5**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\pay\_approval.php

MD5 Hashing algorithm.

$hash = md5($PAY['P\_TID'].$PAY['P\_MID'].$PAY['P\_AMT']);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\pay\_result.php

MD5 Hashing algorithm.

$hash = md5(get\_session('P\_TID').$default['de\_inicis\_mid'].get\_session('P\_AMT'));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\pay\_return.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$oid = isset($\_REQUEST['oid']) ? preg\_replace('/[^0-9a-z\_\-]/i', '', $\_REQUEST['oid']) : '';

**MEDIUM: Potentially Unsafe Code - md5**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\pay\_return.php

MD5 Hashing algorithm.

$hash = md5($PAY['P\_TID'].$PAY['P\_MID'].$PAY['P\_AMT']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\pay\_return.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<form name="forderform" method="post" action="'.$order\_action\_url.'" autocomplete="off">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\pay\_return.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo make\_order\_field($data, $exclude);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\pay\_return.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="hidden" name="res\_cd" value="'.$PAY['P\_STATUS'].'">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\pay\_return.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="hidden" name="P\_HASH" value="'.$hash.'">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\pay\_return.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="hidden" name="P\_TYPE" value="'.$PAY['P\_TYPE'].'">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\pay\_return.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="hidden" name="P\_AUTH\_DT" value="'.$PAY['P\_AUTH\_DT'].'">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\pay\_return.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="hidden" name="P\_VACT\_BANK" value="'.$PAY['P\_FN\_NM'].'">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\pay\_return.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="hidden" name="P\_AUTH\_NO" value="'.$PAY['P\_AUTH\_NO'].'">'.PHP\_EOL;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\settle\_common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$P\_OID = isset($\_POST['P\_OID']) ? preg\_replace("/[ #\&\+%@=\/\\\:;,\.'\"\^`~|\!\?\\*$#<>()\[\]\{\}]/i", "", $\_POST['P\_OID']) : '';

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\settle\_common.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

sql\_query(" ALTER TABLE `{$g5['g5\_shop\_inicis\_log\_table']}`

**MEDIUM: Potentially Unsafe Code - md5**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\settle\_common.php

MD5 Hashing algorithm.

$\_POST['P\_HASH'] = md5(get\_session('P\_TID').$default['de\_inicis\_mid'].$P\_AMT);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\settle\_common.php

MD5 Hashing algorithm.

set\_session('ss\_personalpay\_hash', md5($P\_OID.$P\_AMT.$pp\_time['pp\_time']));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\settle\_common.php

MD5 Hashing algorithm.

$hash = md5($PAY['P\_TID'].$PAY['P\_MID'].$PAY['P\_AMT']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 276 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\settle\_common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $receipt\_time);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 377 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\settle\_common.php

if(!($fp = fopen($path.$file, "a+"))) return 0;

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 377 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\settle\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if(!($fp = fopen($path.$file, "a+"))) return 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 380 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\settle\_common.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

print\_r($msg);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 384 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\inicis\settle\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if(fwrite($fp, " ".$ob\_msg."\n") === FALSE)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\easypay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_name" value="<?php echo $goods; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\easypay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_mny" value="<?php echo $tot\_price ?>" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\easypay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ordr\_idxx" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\easypay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bask\_cntx" value="<?php echo (int)$goods\_count + 1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\easypay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_info" value="<?php echo $good\_info; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\easypay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="param\_opt\_1" value="<?php echo get\_text($param\_opt\_1); ?>"/>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\easypay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="param\_opt\_2" value="<?php echo get\_text($param\_opt\_2); ?>"/>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\easypay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="param\_opt\_3" value="<?php echo get\_text($param\_opt\_3); ?>"/>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\easypay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="tablet\_size" value="<?php echo $tablet\_size; ?>"/>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\easypay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="kcp\_noint" value="<?php echo ($default['de\_card\_noint\_use'] ? '' : 'N'); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\easypay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_tax\_mny" value="<?php echo $comm\_tax\_mny; ?>"> <!-- 과세금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\easypay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_vat\_mny" value="<?php echo $comm\_vat\_mny; ?>"> <!-- 부가세 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\easypay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_free\_mny" value="<?php echo $comm\_free\_mny; ?>"> <!-- 비과세 금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\easypay\_form.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_tax\_mny" value="<?php echo $comm\_tax\_mny; ?>"> <!-- 과세금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\easypay\_form.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_vat\_mny" value="<?php echo $comm\_vat\_mny; ?>"> <!-- 부가세 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\easypay\_form.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_free\_mny" value="<?php echo $comm\_free\_mny; ?>"> <!-- 비과세 금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\m\_order.script.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

nhnkcp\_pay\_form.good\_info.value = "<?php echo $good\_info; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_name" value="<?php echo $goods; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_mny" value="<?php echo $tot\_price ?>" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ordr\_idxx" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bask\_cntx" value="<?php echo (int)$goods\_count + 1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_info" value="<?php echo $good\_info; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="param\_opt\_1" value="<?php echo get\_text($param\_opt\_1); ?>"/>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="param\_opt\_2" value="<?php echo get\_text($param\_opt\_2); ?>"/>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="param\_opt\_3" value="<?php echo get\_text($param\_opt\_3); ?>"/>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="tablet\_size" value="<?php echo $tablet\_size; ?>"/>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="kcp\_noint" value="<?php echo ($default['de\_card\_noint\_use'] ? '' : 'N'); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_tax\_mny" value="<?php echo $comm\_tax\_mny; ?>"> <!-- 과세금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_vat\_mny" value="<?php echo $comm\_vat\_mny; ?>"> <!-- 부가세 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_free\_mny" value="<?php echo $comm\_free\_mny; ?>"> <!-- 비과세 금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_tax\_mny" value="<?php echo $comm\_tax\_mny; ?>"> <!-- 과세금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_vat\_mny" value="<?php echo $comm\_vat\_mny; ?>"> <!-- 부가세 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_free\_mny" value="<?php echo $comm\_free\_mny; ?>"> <!-- 비과세 금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\orderform.3.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="site\_cd" value="<?php echo $default['de\_kcp\_mid']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\orderform.3.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <?php if ($default['de\_card\_use'] || $default['de\_iche\_use']) { echo "결제대행사 : KCP"; } ?> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.location.href = "<?php echo $js\_return\_url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 199 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.location.href = "<?php echo $js\_return\_url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 205 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.location.href = "<?php echo $js\_return\_url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 243 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<form name="forderform" method="post" action="'.$order\_action\_url.'" autocomplete="off">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 245 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo make\_order\_field($data, $exclude);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 248 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="hidden" name="'.$key.'" value="'.$value.'">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 257 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_name" value="<?php echo $good\_name; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 258 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_mny" value="<?php echo $good\_mny; ?>" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 259 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name='buyr\_name' value="<?php echo $buyr\_name; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 260 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="buyr\_tel1" value="<?php echo $buyr\_tel1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 261 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="buyr\_tel2" value="<?php echo $buyr\_tel2; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 262 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="buyr\_mail" value="<?php echo $buyr\_mail; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 270 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="payco\_direct" value="<?php echo $payco\_direct; ?>"> <!-- PAYCO 결제창 호출 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 273 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="naverpay\_direct" value="<?php echo $naverpay\_direct; ?>"> <!-- 네이버페이 결제창 호출 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 279 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="kakaopay\_direct" value="<?php echo $kakaopay\_direct; ?>"> <!-- 카카오페이 결제창 호출 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 287 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="site\_cd" value="<?php echo $g\_conf\_site\_cd; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 289 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="shop\_name" value="<?php echo $g\_conf\_site\_name; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 291 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="pay\_method" value="<?php echo $pay\_method; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 293 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ordr\_idxx" value="<?php echo $ordr\_idxx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 304 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ActionResult" value="<?php echo $ActionResult; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 306 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="escw\_used" value="<?php echo $escw\_used; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 308 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="pay\_mod" value="<?php echo ($default['de\_escrow\_use']?'O':'N'); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 310 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="rcvr\_name" value="<?php echo $rcvr\_name; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 312 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="rcvr\_tel1" value="<?php echo $rcvr\_tel1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 314 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="rcvr\_tel2" value="<?php echo $rcvr\_tel2; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 316 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="rcvr\_add1" value="<?php echo $rcvr\_add1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 318 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="rcvr\_add2" value="<?php echo $rcvr\_add2; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 320 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="rcvr\_mail" value="<?php echo $rcvr\_mail; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 322 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="rcvr\_zipx" value="<?php echo $rcvr\_zipx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 324 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bask\_cntx" value="<?php echo $bask\_cntx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 326 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_info" value="<?php echo $good\_info; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 330 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="param\_opt\_1" value="<?php echo get\_text($param\_opt\_1); ?>"/>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 331 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="param\_opt\_2" value="<?php echo get\_text($param\_opt\_2); ?>"/>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 332 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="param\_opt\_3" value="<?php echo get\_text($param\_opt\_3); ?>"/>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 336 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="tablet\_size" value="<?php echo $tablet\_size; ?>"/>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 354 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="kcp\_noint" value="<?php echo ($default['de\_card\_noint\_use'] ? '' : 'N'); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 369 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_tax\_mny" value="<?php echo $comm\_tax\_mny; ?>"> <!-- 과세금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 370 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_vat\_mny" value="<?php echo $comm\_vat\_mny; ?>"> <!-- 부가세 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 371 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_free\_mny" value="<?php echo $comm\_free\_mny; ?>"> <!-- 비과세 금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 376 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="res\_cd" value="<?php echo $res\_cd; ?>"> <!-- 결과 코드 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 377 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="tran\_cd" value="<?php echo $tran\_cd; ?>"> <!-- 트랜잭션 코드 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 378 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="enc\_info" value="<?php echo $enc\_info; ?>"> <!-- 암호화 정보 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 379 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="enc\_data" value="<?php echo $enc\_data; ?>"> <!-- 암호화 데이터 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 384 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\order\_approval\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $js\_return\_url; ?>">돌아가기</a>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\pp\_ax\_hub.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$tran\_cd = isset($\_POST["tran\_cd"]) ? preg\_replace('/[^0-9A-Za-z\_\-\.]/i', '', $\_POST["tran\_cd"]) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\pp\_ax\_hub.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ordr\_idxx = isset($\_POST["ordr\_idxx"]) ? preg\_replace('/[^0-9A-Za-z\_\-\.]/i', '', $\_POST["ordr\_idxx"]) : '';

**STANDARD: Potentially Unsafe Code - exec**

Line: 292 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\pp\_ax\_hub\_lib.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$rt = exec( $exec\_cmd );

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 292 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\kcp\pp\_ax\_hub\_lib.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

$rt = exec( $exec\_cmd );

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\mispwapurl.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "LGD\_OID = ".$LGD\_OID;

**MEDIUM: Potentially Unsafe Code - md5**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\note\_url.php

MD5 Hashing algorithm.

$LGD\_HASHDATA2 = md5($LGD\_MID.$LGD\_OID.$LGD\_AMOUNT.$LGD\_RESPCODE.$LGD\_TIMESTAMP.$LGD\_MERTKEY);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\note\_url.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $resultMSG;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="LGD\_OID" id="LGD\_OID" value="<?php echo $od\_id; ?>"> <!-- 주문번호 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="LGD\_PRODUCTINFO" id="LGD\_PRODUCTINFO" value="<?php echo $goods; ?>"> <!-- 상품정보 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="LGD\_TAXFREEAMOUNT" id="LGD\_TAXFREEAMOUNT" value="<?php echo $comm\_free\_mny; ?>"> <!-- 결제금액 중 면세금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="LGD\_BUYERID" id="LGD\_BUYERID" value="<?php echo $LGD\_BUYERID; ?>"> <!-- 구매자ID -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_mny" value="<?php echo $tot\_price ?>" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_mny" value="<?php echo $tot\_price ?>" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_tax\_mny" value="<?php echo $comm\_tax\_mny; ?>"> <!-- 과세금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_vat\_mny" value="<?php echo $comm\_vat\_mny; ?>"> <!-- 부가세 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_free\_mny" value="<?php echo $comm\_free\_mny; ?>"> <!-- 비과세 금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\returnurl.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<form name="forderform" method="post" action="'.$order\_action\_url.'" autocomplete="off">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\returnurl.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo make\_order\_field($data, $exclude);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\returnurl.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="hidden" name="res\_cd" value="'.$LGD\_RESPCODE.'">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\returnurl.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="hidden" name="LGD\_PAYKEY" value="'.$LGD\_PAYKEY.'">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - md5**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\xpay\_approval.php

MD5 Hashing algorithm.

$LGD\_HASHDATA = md5($LGD\_MID.$LGD\_OID.$LGD\_AMOUNT.$LGD\_TIMESTAMP.$xpay->config[$LGD\_MID]);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\xpay\_approval.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var LGD\_window\_type = '<?php echo $CST\_WINDOW\_TYPE; ?>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\xpay\_approval.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

lgdwin = open\_paymentwindow(document.getElementById('LGD\_PAYINFO'), '<?php echo $CST\_PLATFORM; ?>', LGD\_window\_type);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\lg\xpay\_approval.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo'"<input type="hidden" name="'.$key.'" id="'.$key.'" value="'.$value.'">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\samsungpay\order.script.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

samsungpayform.P\_RETURN\_URL.value = "<?php echo $return\_url.$od\_id; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\samsungpay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_OID" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\samsungpay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_GOODS" value="<?php echo $goods; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\samsungpay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_AMT" value="<?php echo $tot\_price; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\samsungpay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_MID" value="<?php echo $default['de\_inicis\_mid']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\samsungpay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_NEXT\_URL" value="<?php echo $next\_url; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\samsungpay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_NOTI\_URL" value="<?php echo $noti\_url; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\samsungpay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_RESERVED" value="bank\_receipt=N&twotrs\_isp=Y&block\_isp=Y<?php echo $useescrow; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\samsungpay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="DEF\_RESERVED" value="bank\_receipt=N&twotrs\_isp=Y&block\_isp=Y<?php echo $useescrow; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\samsungpay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_NOTI" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\samsungpay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_mny" value="<?php echo $tot\_price; ?>" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\shop\samsungpay\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_mny" value="<?php echo $tot\_price ?>" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<ul class="<?php echo isset($view) ? 'view\_is\_list btn\_top' : 'btn\_top top btn\_bo\_user';?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($admin\_href) { ?><li><a href="<?php echo $admin\_href ?>" class="btn\_admin btn" title="관리자"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($rss\_href) { ?><li><a href="<?php echo $rss\_href ?>" class="btn\_b03 btn" title="RSS"><i class="fa fa-rss" aria-hidden="true"></i><span class="sound\_only">RSS</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="fix\_btn write\_btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo ($board['bo\_mobile\_subject'] ? $board['bo\_mobile\_subject'] : $board['bo\_subject']) ?> 카테고리</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php if ($list[$i]['is\_notice']) echo "bo\_notice"; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_wr\_id[]" value="<?php echo $list[$i]['wr\_id'] ?>" id="chk\_wr\_id\_<?php echo $i ?>" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_wr\_id\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<b class="sound\_only"><?php echo $list[$i]['subject'] ?></b>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['ca\_name\_href'] ?>" class="bo\_cate\_link"><?php echo $list[$i]['ca\_name']; ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['href'] ?>" class="bo\_subject">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['icon\_reply']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (isset($list[$i]['icon\_secret'])) echo $list[$i]['icon\_secret']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['subject'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_hot'])) echo $list[$i]['icon\_hot'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_file'])) echo $list[$i]['icon\_file'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_link'])) echo $list[$i]['icon\_link'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['comment\_cnt']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자</span><?php echo $list[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_date"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$i]['datetime2'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_view"><i class="fa fa-eye" aria-hidden="true"></i> <?php echo number\_format($list[$i]['wr\_hit']) ?><span class="sound\_only">회</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_good) { ?><span class="sound\_only">추천</span><i class="fa fa-thumbs-o-up" aria-hidden="true"></i> <?php echo $list[$i]['wr\_good'] ?><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_nogood) { ?><span class="sound\_only">비추천</span><i class="fa fa-thumbs-o-down" aria-hidden="true"></i> <?php echo $list[$i]['wr\_nogood'] ?><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (count($list) == 0) { echo '<li class="empty\_table">게시물이 없습니다.</li>'; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>전체 <?php echo number\_format($total\_count) ?>건</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $page ?> 페이지

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_board\_sfl\_select\_options($sfl); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input name="stx" value="<?php echo stripslashes($stx) ?>" placeholder="검색어를 입력하세요" required id="stx" class="sch\_input" size="15" maxlength="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- 게시판 이름 표시 <div id="bo\_v\_table"><?php echo ($board['bo\_mobile\_subject'] ? $board['bo\_mobile\_subject'] : $board['bo\_subject']); ?></div> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($scrap\_href) { ?><a href="<?php echo $scrap\_href; ?>" target="\_blank" class=" btn\_scrap" onclick="win\_scrap(this.href); return false;" title="스크랩"><i class="fa fa-thumb-tack" aria-hidden="true"></i><span class="sound\_only">스크랩</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b03 btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($reply\_href) { ?><li><a href="<?php echo $reply\_href ?>"><i class="fa fa-reply" aria-hidden="true"></i> 답변</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($update\_href) { ?><li><a href="<?php echo $update\_href ?>"><i class="fa fa-pencil-square-o" aria-hidden="true"></i> 수정</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($delete\_href) { ?><li><a href="<?php echo $delete\_href ?>" onclick="del(this.href); return false;"><i class="fa fa-trash-o" aria-hidden="true"></i> 삭제</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($copy\_href) { ?><li><a href="<?php echo $copy\_href ?>" onclick="board\_move(this.href); return false;"><i class="fa fa-files-o" aria-hidden="true"></i> 복사</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($move\_href) { ?><li><a href="<?php echo $move\_href ?>" onclick="board\_move(this.href); return false;"><i class="fa fa-arrows" aria-hidden="true"></i> 이동</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($search\_href) { ?><li><a href="<?php echo $search\_href ?>">검색</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $list\_href ?>" class="btn\_list"><i class="fa fa-list" aria-hidden="true"></i> 목록</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="bo\_v" style="width:<?php echo $width; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_cate"><?php echo $view['ca\_name'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_tit"><?php echo cut\_str(get\_text($view['wr\_subject']), 70);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자 </span><?php echo $view['name'] ?><span class="ip"><?php if ($is\_ip\_view) { echo "&nbsp;($ip)"; } ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성일</span><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo date("y-m-d H:i", strtotime($view['wr\_datetime'])) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">조회</span><strong><i class="fa fa-eye" aria-hidden="true"></i> <?php echo number\_format($view['wr\_hit']) ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">댓글</span><strong><i class="fa fa-commenting-o" aria-hidden="true"></i> <?php echo number\_format($view['wr\_comment']) ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_file\_thumbnail($view\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="bo\_v\_con"><?php echo get\_view\_thumbnail($view['content']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_signature) { ?><p><?php echo $signature ?></p><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $good\_href.'&amp;'.$qstr ?>" id="good\_button" class="bo\_v\_good"><i class="fa fa-thumbs-o-up" aria-hidden="true"></i> <span class="sound\_only">추천</span><strong><?php echo number\_format($view['wr\_good']) ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $nogood\_href.'&amp;'.$qstr ?>" id="nogood\_button" class="bo\_v\_nogood"><i class="fa fa-thumbs-o-down" aria-hidden="true"></i> <span class="sound\_only">비추천</span><strong><?php echo number\_format($view['wr\_nogood']) ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($board['bo\_use\_good']) { ?><span class="bo\_v\_good"><i class="fa fa-thumbs-o-up" aria-hidden="true"></i><span class="sound\_only">추천</span><strong><?php echo number\_format($view['wr\_good']) ?></strong></span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($board['bo\_use\_nogood']) { ?><span class="bo\_v\_nogood"><i class="fa fa-thumbs-o-down" aria-hidden="true"></i><span class="sound\_only">비추천</span> <strong><?php echo number\_format($view['wr\_nogood']) ?></strong></span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['file'][$i]['href']; ?>" class="view\_file\_download">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $view['file'][$i]['source'] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $view['file'][$i]['content'] ?> (<?php echo $view['file'][$i]['size'] ?>)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_file\_cnt"><?php echo $view['file'][$i]['download'] ?>회 다운로드</span> |

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>DATE : <?php echo $view['file'][$i]['datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['link\_href'][$i] ?>" target="\_blank">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $link ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_link\_cnt"><?php echo $view['link\_hit'][$i] ?>회 연결</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 193 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($prev\_href) { ?><li class="bo\_v\_prev"><a href="<?php echo $prev\_href ?>"><i class="fa fa-chevron-up" aria-hidden="true"></i><span class="sound\_only">이전글</span> <?php echo $prev\_wr\_subject;?></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 194 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($next\_href) { ?><li class="bo\_v\_next"><a href="<?php echo $next\_href ?>"><i class="fa fa-chevron-down" aria-hidden="true"></i><span class="sound\_only">다음글</span> <?php echo $next\_wr\_subject;?></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 214 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var msg = "파일을 다운로드 하시면 포인트가 차감(<?php echo number\_format($board['bo\_download\_point']) ?>점)됩니다.\n\n포인트는 게시물당 한번만 차감되며 다음에 다시 다운로드 하셔도 중복하여 차감하지 않습니다.\n\n그래도 다운로드 하시겠습니까?";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_min = parseInt(<?php echo $comment\_min ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_max = parseInt(<?php echo $comment\_max ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="bo\_vc\_tit">댓글목록 <span><?php echo $view['wr\_comment']; ?></span></h2>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace("/\[\<a\s.\*href\=\"(http|https|ftp|mms)\:\/\/([^[:space:]]+)\.(mp3|wma|wmv|asf|asx|mpg|mpeg)\".\*\<\/a\>\]/i", "<script>doc\_write(obj\_movie('$1:

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="c\_<?php echo $comment\_id ?>" <?php if ($cmt\_depth) { ?>style="margin-left:<?php echo $cmt\_depth ?>px;border-bottom-color:#f8f8f8"<?php } ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo get\_text($list[$i]['wr\_name']); ?>님의 댓글<?php if ($cmt\_depth) { ?><span class="sound\_only">의 댓글</span><?php } ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_vc\_hdinfo">(<?php echo $list[$i]['ip']; ?>)</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_vc\_hdinfo"><i class="fa fa-clock-o" aria-hidden="true"></i> <time datetime="<?php echo date('Y-m-d\TH:i:s+09:00', strtotime($list[$i]['datetime'])) ?>"><?php echo $list[$i]['datetime'] ?></time></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_reply']) { ?><li><a href="<?php echo $c\_reply\_href; ?>" onclick="comment\_box('<?php echo $comment\_id ?>', 'c'); return false;">답변</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_edit']) { ?><li><a href="<?php echo $c\_edit\_href; ?>" onclick="comment\_box('<?php echo $comment\_id ?>', 'cu'); return false;">수정</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_del']) { ?><li><a href="<?php echo $list[$i]['del\_link']; ?>" onclick="return comment\_delete();">삭제</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (strstr($list[$i]['wr\_option'], "secret")) echo "<img src=\"".$board\_skin\_url."/img/icon\_secret.gif\" alt=\"비밀글\">"; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="edit\_<?php echo $comment\_id ?>"></span><!-- 수정 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="reply\_<?php echo $comment\_id ?>"></span><!-- 답변 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="secret\_comment\_<?php echo $comment\_id ?>" value="<?php echo strstr($list[$i]['wr\_option'],"secret") ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea id="save\_comment\_<?php echo $comment\_id ?>" style="display:none"><?php echo get\_text($list[$i]['content1'], 0) ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fviewcomment" id="fviewcomment" action="<?php echo $comment\_action\_url; ?>" onsubmit="return fviewcomment\_submit(this);" method="post" autocomplete="off" class="bo\_vc\_w">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>" id="w">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comment\_id" value="<?php echo $c\_id ?>" id="comment\_id">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($comment\_min || $comment\_max) { ?>onkeyup="check\_byte('wr\_content', 'char\_count');"<?php } ?> placeholder="댓글내용을 입력해주세요"><?php echo $c\_wr\_content; ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_html; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 254 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($is\_guest) echo chk\_captcha\_js(); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 325 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

"<?php echo G5\_SNS\_URL; ?>/view\_comment\_write.sns.skin.php?bo\_table=<?php echo $bo\_table; ?>",

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fwrite" id="fwrite" action="<?php echo $action\_url ?>" onsubmit="return fwrite\_submit(this);" method="post" enctype="multipart/form-data" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_hidden;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="sound\_only"><?php echo $g5['title'] ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_name" value="<?php echo $name ?>" id="wr\_name" required class="frm\_input full\_input required" maxlength="20" placeholder="이름">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="password" name="wr\_password" id="wr\_password" <?php echo $password\_required ?> class="frm\_input full\_input <?php echo $password\_required ?>" maxlength="20" placeholder="비밀번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="email" name="wr\_email" value="<?php echo $email ?>" id="wr\_email" class="frm\_input full\_input" maxlength="100" placeholder="이메일">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_homepage" value="<?php echo $homepage ?>" id="wr\_homepage" class="frm\_input full\_input" placeholder="홈페이지">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_subject" value="<?php echo $subject ?>" id="wr\_subject" required class="frm\_input full\_input required" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p id="char\_count\_desc">이 게시판은 최소 <strong><?php echo $write\_min; ?></strong>글자 이상, 최대 <strong><?php echo $write\_max; ?></strong>글자 이하까지 글을 쓰실 수 있습니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="wr\_link<?php echo $i ?>"><i class="fa fa-link" aria-hidden="true"></i> <span class="sound\_only">링크 #<?php echo $i ?></span></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_link<?php echo $i ?>" value="<?php if($w=="u"){echo $write['wr\_link'.$i];} ?>" id="wr\_link<?php echo $i ?>" class="frm\_input wr\_link" placeholder="링크를 입력하세요">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bf\_file\_<?php echo $i+1 ?>"><i class="fa fa-download lb\_icon" aria-hidden="true"></i><span class="sound\_only">파일 #<?php echo $i+1 ?></span><span class="btn\_file">파일첨부</span></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="file" name="bf\_file[]" id="bf\_file\_<?php echo $i+1 ?>" title="파일첨부 <?php echo $i+1 ?> : 용량 <?php echo $upload\_max\_filesize ?> 이하만 업로드 가능" class="frm\_file uploadBtn">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bf\_content[]" value="<?php echo ($w == 'u') ? $file[$i]['bf\_content'] : ''; ?>" title="파일 설명을 입력해주세요." class="full\_input frm\_input" size="50" placeholder="파일 설명을 입력해주세요.">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="bf\_file\_del<?php echo $i ?>" name="bf\_file\_del[<?php echo $i; ?>]" value="1"> <label for="bf\_file\_del<?php echo $i ?>"><?php echo $file[$i]['source'].'('.$file[$i]['size'].')'; ?> 파일 삭제</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_html ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="btn\_cancel">취소</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_min = parseInt(<?php echo $write\_min; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_max = parseInt(<?php echo $write\_max; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<ul class="<?php echo isset($view) ? 'view\_is\_list btn\_top' : 'btn\_top top btn\_bo\_user';?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($admin\_href) { ?><li><a href="<?php echo $admin\_href ?>" class="btn\_admin btn" title="관리자"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($rss\_href) { ?><li><a href="<?php echo $rss\_href ?>" class="btn\_b03 btn" title="RSS"><i class="fa fa-rss" aria-hidden="true"></i><span class="sound\_only">RSS</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="fix\_btn write\_btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo ($board['bo\_mobile\_subject'] ? $board['bo\_mobile\_subject'] : $board['bo\_subject']) ?> 카테고리</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_wr\_id[]" value="<?php echo $list[$i]['wr\_id'] ?>" id="chk\_wr\_id\_<?php echo $i ?>" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_wr\_id\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<b class="sound\_only"><?php echo $list[$i]['subject'] ?></b>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['num'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['href'] ?>" class="gall\_img">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo run\_replace('thumb\_image\_tag', $img\_content, $thumb);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['ca\_name\_href'] ?>" class="bo\_cate\_link"><?php echo $list[$i]['ca\_name'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['href'] ?>" class="gall\_li\_tit">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (isset($list[$i]['icon\_secret'])) echo $list[$i]['icon\_secret']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['subject'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['comment\_cnt']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_hot'])) echo $list[$i]['icon\_hot'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자 </span><?php echo $list[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성일 </span><span class="date"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$i]['datetime2'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">조회 </span><strong><i class="fa fa-eye" aria-hidden="true"></i> <?php echo $list[$i]['wr\_hit'] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_good) { ?><span class="sound\_only">추천</span><strong><i class="fa fa-thumbs-o-up" aria-hidden="true"></i> <?php echo $list[$i]['wr\_good'] ?></strong><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_nogood) { ?><span class="sound\_only">비추천</span><strong><i class="fa fa-thumbs-o-down" aria-hidden="true"></i> <?php echo $list[$i]['wr\_nogood'] ?></strong><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (count($list) == 0) { echo "<li class=\"empty\_list\">게시물이 없습니다.</li>"; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>전체 <?php echo number\_format($total\_count) ?>건</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 160 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $page ?> 페이지

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_board\_sfl\_select\_options($sfl); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input name="stx" value="<?php echo stripslashes($stx) ?>" placeholder="검색어를 입력하세요" required id="stx" class="sch\_input" size="15" maxlength="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- 게시판 이름 표시 <div id="bo\_v\_table"><?php echo ($board['bo\_mobile\_subject'] ? $board['bo\_mobile\_subject'] : $board['bo\_subject']); ?></div> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($scrap\_href) { ?><a href="<?php echo $scrap\_href; ?>" target="\_blank" class=" btn\_scrap" onclick="win\_scrap(this.href); return false;" title="스크랩"><i class="fa fa-thumb-tack" aria-hidden="true"></i><span class="sound\_only">스크랩</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b03 btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($reply\_href) { ?><li><a href="<?php echo $reply\_href ?>"><i class="fa fa-reply" aria-hidden="true"></i> 답변</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($update\_href) { ?><li><a href="<?php echo $update\_href ?>"><i class="fa fa-pencil-square-o" aria-hidden="true"></i> 수정</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($delete\_href) { ?><li><a href="<?php echo $delete\_href ?>" onclick="del(this.href); return false;"><i class="fa fa-trash-o" aria-hidden="true"></i> 삭제</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($copy\_href) { ?><li><a href="<?php echo $copy\_href ?>" onclick="board\_move(this.href); return false;"><i class="fa fa-files-o" aria-hidden="true"></i> 복사</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($move\_href) { ?><li><a href="<?php echo $move\_href ?>" onclick="board\_move(this.href); return false;"><i class="fa fa-arrows" aria-hidden="true"></i> 이동</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($search\_href) { ?><li><a href="<?php echo $search\_href ?>">검색</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $list\_href ?>" class="btn\_list"><i class="fa fa-list" aria-hidden="true"></i> 목록</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="bo\_v" style="width:<?php echo $width; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_cate"><?php echo $view['ca\_name'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_tit"><?php echo cut\_str(get\_text($view['wr\_subject']), 70);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자 </span><?php echo $view['name'] ?><span class="ip"><?php if ($is\_ip\_view) { echo "&nbsp;($ip)"; } ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성일</span><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo date("y-m-d H:i", strtotime($view['wr\_datetime'])) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">조회</span><strong><i class="fa fa-eye" aria-hidden="true"></i> <?php echo number\_format($view['wr\_hit']) ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">댓글</span><strong><i class="fa fa-commenting-o" aria-hidden="true"></i> <?php echo number\_format($view['wr\_comment']) ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_file\_thumbnail($view\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="bo\_v\_con"><?php echo get\_view\_thumbnail($view['content']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_signature) { ?><p><?php echo $signature ?></p><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $good\_href.'&amp;'.$qstr ?>" id="good\_button" class="bo\_v\_good"><i class="fa fa-thumbs-o-up" aria-hidden="true"></i> <span class="sound\_only">추천</span><strong><?php echo number\_format($view['wr\_good']) ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $nogood\_href.'&amp;'.$qstr ?>" id="nogood\_button" class="bo\_v\_nogood"><i class="fa fa-thumbs-o-down" aria-hidden="true"></i> <span class="sound\_only">비추천</span><strong><?php echo number\_format($view['wr\_nogood']) ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($board['bo\_use\_good']) { ?><span class="bo\_v\_good"><i class="fa fa-thumbs-o-up" aria-hidden="true"></i><span class="sound\_only">추천</span><strong><?php echo number\_format($view['wr\_good']) ?></strong></span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($board['bo\_use\_nogood']) { ?><span class="bo\_v\_nogood"><i class="fa fa-thumbs-o-down" aria-hidden="true"></i><span class="sound\_only">비추천</span> <strong><?php echo number\_format($view['wr\_nogood']) ?></strong></span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['file'][$i]['href']; ?>" class="view\_file\_download">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $view['file'][$i]['source'] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $view['file'][$i]['content'] ?> (<?php echo $view['file'][$i]['size'] ?>)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_file\_cnt"><?php echo $view['file'][$i]['download'] ?>회 다운로드</span> |

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>DATE : <?php echo $view['file'][$i]['datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['link\_href'][$i] ?>" target="\_blank">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $link ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 182 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_link\_cnt"><?php echo $view['link\_hit'][$i] ?>회 연결</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($prev\_href) { ?><li class="bo\_v\_prev"><a href="<?php echo $prev\_href ?>"><i class="fa fa-chevron-up" aria-hidden="true"></i><span class="sound\_only">이전글</span> <?php echo $prev\_wr\_subject;?></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 196 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($next\_href) { ?><li class="bo\_v\_next"><a href="<?php echo $next\_href ?>"><i class="fa fa-chevron-down" aria-hidden="true"></i><span class="sound\_only">다음글</span> <?php echo $next\_wr\_subject;?></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 215 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var msg = "파일을 다운로드 하시면 포인트가 차감(<?php echo number\_format($board['bo\_download\_point']) ?>점)됩니다.\n\n포인트는 게시물당 한번만 차감되며 다음에 다시 다운로드 하셔도 중복하여 차감하지 않습니다.\n\n그래도 다운로드 하시겠습니까?";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_min = parseInt(<?php echo $comment\_min ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_max = parseInt(<?php echo $comment\_max ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="bo\_vc\_tit">댓글목록 <span><?php echo $view['wr\_comment']; ?></span></h2>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace("/\[\<a\s.\*href\=\"(http|https|ftp|mms)\:\/\/([^[:space:]]+)\.(mp3|wma|wmv|asf|asx|mpg|mpeg)\".\*\<\/a\>\]/i", "<script>doc\_write(obj\_movie('$1:

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="c\_<?php echo $comment\_id ?>" <?php if ($cmt\_depth) { ?>style="margin-left:<?php echo $cmt\_depth ?>px;border-bottom-color:#f8f8f8"<?php } ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo get\_text($list[$i]['wr\_name']); ?>님의 댓글<?php if ($cmt\_depth) { ?><span class="sound\_only">의 댓글</span><?php } ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_vc\_hdinfo">(<?php echo $list[$i]['ip']; ?>)</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_vc\_hdinfo"><i class="fa fa-clock-o" aria-hidden="true"></i> <time datetime="<?php echo date('Y-m-d\TH:i:s+09:00', strtotime($list[$i]['datetime'])) ?>"><?php echo $list[$i]['datetime'] ?></time></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_reply']) { ?><li><a href="<?php echo $c\_reply\_href; ?>" onclick="comment\_box('<?php echo $comment\_id ?>', 'c'); return false;">답변</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_edit']) { ?><li><a href="<?php echo $c\_edit\_href; ?>" onclick="comment\_box('<?php echo $comment\_id ?>', 'cu'); return false;">수정</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_del']) { ?><li><a href="<?php echo $list[$i]['del\_link']; ?>" onclick="return comment\_delete();">삭제</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (strstr($list[$i]['wr\_option'], "secret")) echo "<img src=\"".$board\_skin\_url."/img/icon\_secret.gif\" alt=\"비밀글\">"; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="edit\_<?php echo $comment\_id ?>"></span><!-- 수정 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="reply\_<?php echo $comment\_id ?>"></span><!-- 답변 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="secret\_comment\_<?php echo $comment\_id ?>" value="<?php echo strstr($list[$i]['wr\_option'],"secret") ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea id="save\_comment\_<?php echo $comment\_id ?>" style="display:none"><?php echo get\_text($list[$i]['content1'], 0) ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fviewcomment" id="fviewcomment" action="<?php echo $comment\_action\_url; ?>" onsubmit="return fviewcomment\_submit(this);" method="post" autocomplete="off" class="bo\_vc\_w">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>" id="w">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comment\_id" value="<?php echo $c\_id ?>" id="comment\_id">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($comment\_min || $comment\_max) { ?>onkeyup="check\_byte('wr\_content', 'char\_count');"<?php } ?> placeholder="댓글내용을 입력해주세요"><?php echo $c\_wr\_content; ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_html; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 254 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($is\_guest) echo chk\_captcha\_js(); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 325 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

"<?php echo G5\_SNS\_URL; ?>/view\_comment\_write.sns.skin.php?bo\_table=<?php echo $bo\_table; ?>",

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fwrite" id="fwrite" action="<?php echo $action\_url ?>" onsubmit="return fwrite\_submit(this);" method="post" enctype="multipart/form-data" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_hidden;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="sound\_only"><?php echo $g5['title'] ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_name" value="<?php echo $name ?>" id="wr\_name" required class="frm\_input full\_input required" maxlength="20" placeholder="이름">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="password" name="wr\_password" id="wr\_password" <?php echo $password\_required ?> class="frm\_input full\_input <?php echo $password\_required ?>" maxlength="20" placeholder="비밀번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="email" name="wr\_email" value="<?php echo $email ?>" id="wr\_email" class="frm\_input full\_input" maxlength="100" placeholder="이메일">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_homepage" value="<?php echo $homepage ?>" id="wr\_homepage" class="frm\_input full\_input" placeholder="홈페이지">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_subject" value="<?php echo $subject ?>" id="wr\_subject" required class="frm\_input full\_input required" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p id="char\_count\_desc">이 게시판은 최소 <strong><?php echo $write\_min; ?></strong>글자 이상, 최대 <strong><?php echo $write\_max; ?></strong>글자 이하까지 글을 쓰실 수 있습니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="wr\_link<?php echo $i ?>"><i class="fa fa-link" aria-hidden="true"></i> <span class="sound\_only">링크 #<?php echo $i ?></span></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_link<?php echo $i ?>" value="<?php if($w=="u"){echo $write['wr\_link'.$i];} ?>" id="wr\_link<?php echo $i ?>" class="frm\_input wr\_link" placeholder="링크를 입력하세요">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bf\_file\_<?php echo $i+1 ?>"><i class="fa fa-download lb\_icon" aria-hidden="true"></i><span class="sound\_only">파일 #<?php echo $i+1 ?></span><span class="btn\_file">파일첨부</span></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="file" name="bf\_file[]" id="bf\_file\_<?php echo $i+1 ?>" title="파일첨부 <?php echo $i+1 ?> : 용량 <?php echo $upload\_max\_filesize ?> 이하만 업로드 가능" class="frm\_file uploadBtn">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bf\_content[]" value="<?php echo ($w == 'u') ? $file[$i]['bf\_content'] : ''; ?>" title="파일 설명을 입력해주세요." class="full\_input frm\_input" size="50" placeholder="파일 설명을 입력해주세요.">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="bf\_file\_del<?php echo $i ?>" name="bf\_file\_del[<?php echo $i; ?>]" value="1"> <label for="bf\_file\_del<?php echo $i ?>"><?php echo $file[$i]['source'].'('.$file[$i]['size'].')'; ?> 파일 삭제</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_html ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="btn\_cancel">취소</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_min = parseInt(<?php echo $write\_min; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_max = parseInt(<?php echo $write\_max; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\connect\basic\connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $row['total\_cnt'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\connect\basic\current\_connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="crt\_num"><?php echo $list[$i]['num'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\connect\basic\current\_connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="crt\_profile"><?php echo get\_member\_profile\_img($list[$i]['mb\_id']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\connect\basic\current\_connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="crt\_name"><?php echo $list[$i]['name'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\connect\basic\current\_connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="crt\_lct"><?php echo $display\_location ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\content\basic\content.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="ctt" class="ctt\_<?php echo $co\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\content\basic\content.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title']; ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\content\basic\content.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="faq\_hhtml">'.conv\_content($fm['fm\_mobile\_head\_html'], 1).'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fm\_id" value="<?php echo $fm\_id;?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx;?>" required id="stx" class="frm\_input" size="15" maxlength="15">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $category\_href;?>?fm\_id=<?php echo $v['fm\_id']?>" <?php echo $category\_option;?> ><?php echo $category\_msg.$v['fm\_subject'];?></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="faq\_wrap" class="faq\_<?php echo $fm\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $g5['title']; ?> 목록</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="tit\_bg">Q</span><a href="#none" onclick="return faq\_open(this);"><?php echo conv\_content($v['fa\_subject'], 1); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($v['fa\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($page\_rows, $page, $total\_page, $\_SERVER['SCRIPT\_NAME'].'?'.$qstr.'&amp;page='); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="faq\_thtml">'.conv\_content($fm['fm\_mobile\_tail\_html'], 1).'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="lt\_title"><strong><?php echo $bo\_subject; ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="<?php echo $list\_count ? 'latest-sel' : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $echo\_ul;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".$wr\_href."\" class=\"lt\_thumb\">".run\_replace('thumb\_image\_tag', $img\_content, $thumb)."</a> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".$wr\_href."\" class=\"lt\_tit\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_secret']) echo "<i class=\"fa fa-lock\" aria-hidden=\"true\"></i> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strong>".$list[$i]['subject']."</strong>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo " <span class=\"new\_icon\">N</span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_file']) echo " <i class=\"fa fa-download\" aria-hidden=\"true\"></i>" ;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_link']) echo " <i class=\"fa fa-link\" aria-hidden=\"true\"></i>" ;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_hot']) echo " <i class=\"fa fa-heart\" aria-hidden=\"true\"></i>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['comment\_cnt']) echo "

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['datetime'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="page\_print"><b><?php echo $start\_page\_num; ?></b>/<?php echo $start\_page\_num; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="lt\_more"><span class="sound\_only"><?php echo $bo\_subject ?></span>전체보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\comment\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="cm\_lt\_title"><a href="<?php echo get\_pretty\_url($bo\_table); ?>">최신댓글</a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\comment\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="cm\_lt\_nick"><?php echo get\_member\_profile\_img($member['mb\_id']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\comment\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table, $list[$i]['wr\_id']); ?>" class="over"><?php echo $list[$i]['subject']; ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\comment\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="lt\_nick"><?php echo $list[$i]['name'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\comment\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="lt\_date"><?php echo $list[$i]['datetime2'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\comment\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="lt\_more"><span class="sound\_only"><?php echo $bo\_subject ?></span>더보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><a href="<?php echo get\_pretty\_url($bo\_table); ?>"><?php echo $bo\_subject ?></a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_secret']) echo "<span class=\"lock\_icon\"><i class=\"fa fa-lock\" aria-hidden=\"true\"></i></span> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".get\_pretty\_url($bo\_table, $list[$i]['wr\_id'])."\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strong>".$list[$i]['subject']."</strong>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['comment\_cnt'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><a href="<?php echo G5\_BBS\_URL ?>/board.php?bo\_table=<?php echo $bo\_table ?>"><?php echo $bo\_subject ?></a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".$list[$i]['href']."\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strong>".$list[$i]['subject']."</strong>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_new'])) echo " " . $list[$i]['icon\_new'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_BBS\_URL ?>/board.php?bo\_table=<?php echo $bo\_table ?>" class="more\_btn"><span class="sound\_only"><?php echo $bo\_subject ?></span>전체보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\formmail.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $name ?>님께 메일보내기</h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\formmail.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="to" value="<?php echo $email ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\formmail.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fnick" value="<?php echo get\_text($member['mb\_nick']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\formmail.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fmail" value="<?php echo $member['mb\_email'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="flogin" action="<?php echo $login\_action\_url ?>" onsubmit="return flogin\_submit(this);" method="post" id="flogin">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="url" value="<?php echo $login\_url ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($default['de\_guest\_privacy'], $config['cf\_editor']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

f.url.value = "<?php echo $url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

f.action = "<?php echo $url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="forderinquiry" method="post" action="<?php echo urldecode($url); ?>" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_id" value="<?php echo $od\_id; ?>" id="od\_id" required class="frm\_input required" size="20" placeholder="주문서번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fcertrefreshform" id="member\_cert\_refresh" action="<?php echo $action\_url ?>" onsubmit="return fcertrefreshform\_submit(this);" method="POST" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cert\_type" value="<?php echo $member['mb\_certify']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $member['mb\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_hp" value="<?php echo $member['mb\_hp']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_name" value="<?php echo $member['mb\_name']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td>생년월일<?php echo (empty($member['mb\_dupinfo']))? ", 휴대폰 번호(아이핀 제외)" : ""; ?>, 암호화된 개인식별부호(CI)</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

certify\_win\_open("<?php echo $cert\_type; ?>", "<?php echo $cert\_url; ?>" + params);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\member\_confirm.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\member\_confirm.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fmemberconfirm" action="<?php echo $url ?>" onsubmit="return fmemberconfirm\_submit(this);" method="post">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\member\_confirm.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $member['mb\_id'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\member\_confirm.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="mb\_confirm\_id"><?php echo $member['mb\_id'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $g5['title'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="win\_total">전체 <?php echo $kind\_title ?>쪽지 <?php echo $total\_count ?>통<br></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php echo $readed; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($list[$i]['mb\_id']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['name']; ?> <span class="memo\_datetime"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$i]['send\_datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['view\_href'] ?>"><?php echo $memo\_preview; ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['del\_href'] ?>" onclick="del(this.href); return false;" class="memo\_del"><i class="fa fa-trash-o" aria-hidden="true"></i> <span class="sound\_only">삭제</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($i==0) { echo '<li class="empty\_table">자료가 없습니다.</li>'; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p class="win\_desc"><i class="fa fa-info-circle" aria-hidden="true"></i> 쪽지 보관일수는 최장 <strong><?php echo $config['cf\_memo\_del'] ?></strong>일 입니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fmemoform" action="<?php echo $memo\_action\_url; ?>" onsubmit="return fmemoform\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="me\_recv\_mb\_id" value="<?php echo $me\_recv\_mb\_id; ?>" id="me\_recv\_mb\_id" required class="frm\_input full\_input required" size="47" placeholder="받는 회원아이디">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($config['cf\_memo\_send\_point']) { ?><br>쪽지 보낼때 회원당 <?php echo number\_format($config['cf\_memo\_send\_point']); ?>점의 포인트를 차감합니다.<?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="me\_memo" id="me\_memo" required class="required"><?php echo $content ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($mb['mb\_id']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="memo\_view\_nick"><?php echo $nick ?></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="memo\_view\_date"><span class="sound\_only"><?php echo $kind\_date ?>시간</span><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $memo['me\_send\_datetime'] ?></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="memo\_op\_btn list\_btn"><a href="<?php echo $list\_link ?>" class="btn\_b01 btn"><i class="fa fa-list" aria-hidden="true"></i><span class="sound\_only">목록</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="memo\_op\_btn del\_btn"><a href="<?php echo $del\_link; ?>" onclick="del(this.href); return false;" class="memo\_del btn\_b01 btn"><i class="fa fa-trash-o" aria-hidden="true"></i> <span class="sound\_only">삭제</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $prev\_link ?>" class="btn\_left"><i class="fa fa-chevron-left" aria-hidden="true"></i> 이전쪽지</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $next\_link ?>" class="btn\_right">다음쪽지 <i class="fa fa-chevron-right" aria-hidden="true"></i></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($memo['me\_memo'], 0) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($kind == 'recv') { ?><a href="./memo\_form.php?me\_recv\_mb\_id=<?php echo $mb['mb\_id'] ?>&amp;me\_id=<?php echo $memo['me\_id'] ?>" class="reply\_btn">답장</a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fboardpassword" action="<?php echo $action; ?>" method="post">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comment\_id" value="<?php echo $comment\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\password\_lost.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fpasswordlost" action="<?php echo $action\_url ?>" onsubmit="return fpasswordlost\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\password\_lost.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

certify\_win\_open("<?php echo $cert\_type; ?>", "<?php echo $cert\_url; ?>"+params);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\password\_reset.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fpasswordreset" action="<?php echo $action\_url; ?>" onsubmit="return fpasswordreset\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\password\_reset.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_id" id="mb\_id" value="<?php echo $\_POST['mb\_id']; ?>" required class="required frm\_input full\_input" size="30" placeholder="아이디" readonly>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo number\_format($member['mb\_point']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php echo $point\_use\_class; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="point\_tit"><?php echo $po\_content; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="point\_num"><?php if ($point1) echo $point1; else echo $point2; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="point\_date1"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo conv\_date\_format('y-m-d H시', $row['po\_datetime']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="point\_date<?php echo $expr; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

만료 <?php echo substr(str\_replace('-', '', $row['po\_expire\_date']), 2); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php } else echo $row['po\_expire\_date'] == '9999-12-31' ? '&nbsp;' : $row['po\_expire\_date']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $sum\_point1; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $sum\_point2; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, $\_SERVER['SCRIPT\_NAME'].'?'.$qstr.'&amp;page='); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $mb\_nick ?>님의 프로필</h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $mb['mb\_level'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($mb['mb\_point']) ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><a href="<?php echo $mb\_homepage ?>" target="\_blank"><?php echo $mb\_homepage ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo ($member['mb\_level'] >= $mb['mb\_level']) ? substr($mb['mb\_datetime'],0,10) ." (".number\_format($mb\_reg\_after)." 일)" : "알 수 없음"; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo ($member['mb\_level'] >= $mb['mb\_level']) ? $mb['mb\_today\_login'] : "알 수 없음"; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo $mb\_profile ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fregister" id="fregister" action="<?php echo $register\_action\_url ?>" onsubmit="return fregister\_submit(this);" method="POST" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea readonly><?php echo get\_text($config['cf\_stipulation']) ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td>아이디, 이름, 비밀번호<?php echo ($config['cf\_cert\_use'])? ", 생년월일, 휴대폰 번호(본인인증 할 때만, 아이핀 제외), 암호화된 개인식별부호(CI)" : ""; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fregisterform" id="fregisterform" action="<?php echo $register\_action\_url ?>" onsubmit="return fregisterform\_submit(this);" method="post" enctype="multipart/form-data" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="agree" value="<?php echo $agree ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="agree2" value="<?php echo $agree2 ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cert\_type" value="<?php echo $member['mb\_certify']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (isset($member['mb\_sex'])) { ?><input type="hidden" name="mb\_sex" value="<?php echo $member['mb\_sex'] ?>"><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_nick\_default" value="<?php echo get\_text($member['mb\_nick']) ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_nick" value="<?php echo get\_text($member['mb\_nick']) ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_id" value="<?php echo $member['mb\_id'] ?>" id="reg\_mb\_id" class="frm\_input full\_input <?php echo $required ?> <?php echo $readonly ?>" minlength="3" maxlength="20" <?php echo $required ?> <?php echo $readonly ?> placeholder="아이디 (필수)">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="password" name="mb\_password" id="reg\_mb\_password" class="frm\_input full\_input <?php echo $required ?>" minlength="3" maxlength="20" <?php echo $required ?> placeholder="비밀번호 (필수)">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="password" name="mb\_password\_re" id="reg\_mb\_password\_re" class="frm\_input full\_input <?php echo $required ?>" minlength="3" maxlength="20" <?php echo $required ?> placeholder="비밀번호확인 (필수)">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $mb\_cert; ?> 본인확인</strong><?php if ($member['mb\_adult']) { ?> 및 <strong>성인인증</strong><?php } ?> 완료

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="reg\_mb\_name" class="sound\_only">이름 (필수)<?php echo $desc\_name ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" id="reg\_mb\_name" name="mb\_name" value="<?php echo get\_text($member['mb\_name']) ?>" <?php echo $required ?> <?php echo $name\_readonly; ?> class="frm\_input full\_input <?php echo $required ?> <?php echo $name\_readonly ?>" placeholder="이름 (필수)<?php echo $desc\_name ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

닉네임을 바꾸시면 앞으로 <?php echo (int)$config['cf\_nick\_modify'] ?>일 이내에는 변경 할 수 없습니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_nick\_default" value="<?php echo isset($member['mb\_nick'])?get\_text($member['mb\_nick']):''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_nick" value="<?php echo isset($member['mb\_nick'])?get\_text($member['mb\_nick']):''; ?>" id="reg\_mb\_nick" required class="frm\_input full\_input required nospace" maxlength="20" placeholder="닉네임 (필수)">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($w=='') { echo "E-mail 로 발송된 내용을 확인한 후 인증하셔야 회원가입이 완료됩니다."; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($w=='u') { echo "E-mail 주소를 변경하시면 다시 인증하셔야 합니다."; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="old\_email" value="<?php echo $member['mb\_email'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="email" name="mb\_email" value="<?php echo isset($member['mb\_email'])?$member['mb\_email']:''; ?>" id="reg\_mb\_email" required class="frm\_input email required" size="50" maxlength="100" placeholder="E-mail (필수)">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_homepage" value="<?php echo get\_text($member['mb\_homepage']) ?>" id="reg\_mb\_homepage" class="frm\_input full\_input <?php echo $config['cf\_req\_homepage']?"required":""; ?>" maxlength="255" <?php echo $config['cf\_req\_homepage']?"required":""; ?> placeholder="홈페이지<?php if ($config['cf\_req\_homepage']){ ?> (필수)<?php } ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_tel" value="<?php echo get\_text($member['mb\_tel']) ?>" id="reg\_mb\_tel" class="frm\_input full\_input <?php echo $config['cf\_req\_tel']?"required":""; ?>" <?php if ($config['cf\_cert\_use'] && ($config['cf\_cert\_hp'] || $config['cf\_cert\_simple']) && $member['mb\_certify']) { echo "readonly"; } ?> maxlength="20" <?php echo $config['cf\_req\_tel']?"required":""; ?> placeholder="전화번호<?php if ($config['cf\_req\_tel']) { ?> (필수)<?php } ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="reg\_mb\_hp" class="sound\_only">휴대폰번호<?php if (!empty($hp\_required)) { ?> (필수)<?php } ?><?php echo $desc\_phone ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_hp" value="<?php echo get\_text($member['mb\_hp']) ?>" id="reg\_mb\_hp" <?php echo $hp\_required; ?> <?php echo $hp\_readonly; ?> class="frm\_input full\_input <?php echo $hp\_required; ?> <?php echo $hp\_readonly; ?>" maxlength="20" placeholder="휴대폰번호<?php if (!empty($hp\_required)) { ?> (필수)<?php } ?><?php echo $desc\_phone ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="old\_mb\_hp" value="<?php echo get\_text($member['mb\_hp']) ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="reg\_mb\_zip" class="sound\_only">우편번호<?php echo $config['cf\_req\_addr']?' (필수)':''; ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_zip" value="<?php echo $member['mb\_zip1'].$member['mb\_zip2']; ?>" id="reg\_mb\_zip" <?php echo $config['cf\_req\_addr']?"required":""; ?> class="frm\_input <?php echo $config['cf\_req\_addr']?"required":""; ?>" size="5" maxlength="6" placeholder="우편번호<?php echo $config['cf\_req\_addr']?' (필수)':''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="reg\_mb\_addr1" class="sound\_only">주소<?php echo $config['cf\_req\_addr']?' (필수)':''; ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_addr1" value="<?php echo get\_text($member['mb\_addr1']) ?>" id="reg\_mb\_addr1" <?php echo $config['cf\_req\_addr']?"required":""; ?> class="frm\_input frm\_address <?php echo $config['cf\_req\_addr']?"required":""; ?>" size="50" placeholder="주소<?php echo $config['cf\_req\_addr']?' (필수)':''; ?>"><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_addr2" value="<?php echo get\_text($member['mb\_addr2']) ?>" id="reg\_mb\_addr2" class="frm\_input frm\_address" size="50" placeholder="상세주소">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 160 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_addr3" value="<?php echo get\_text($member['mb\_addr3']) ?>" id="reg\_mb\_addr3" class="frm\_input frm\_address" size="50" readonly="readonly" placeholder="참고항목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_addr\_jibeon" value="<?php echo get\_text($member['mb\_addr\_jibeon']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 174 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="mb\_signature" id="reg\_mb\_signature" class="<?php echo $config['cf\_req\_signature']?"required":""; ?>" <?php echo $config['cf\_req\_signature']?"required":""; ?> placeholder="서명<?php if ($config['cf\_req\_signature']){ ?> (필수)<?php } ?>"><?php echo $member['mb\_signature'] ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 181 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="mb\_profile" id="reg\_mb\_profile" class="<?php echo $config['cf\_req\_profile']?"required":""; ?>" <?php echo $config['cf\_req\_profile']?"required":""; ?> placeholder="자기소개"><?php echo $member['mb\_profile'] ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 191 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

이미지 크기는 가로 <?php echo $config['cf\_member\_icon\_width'] ?>픽셀, 세로 <?php echo $config['cf\_member\_icon\_height'] ?>픽셀 이하로 해주세요.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 192 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

gif, jpg, png파일만 가능하며 용량 <?php echo number\_format($config['cf\_member\_icon\_size']) ?>바이트 이하만 등록됩니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<img src="<?php echo $mb\_icon\_url ?>" alt="회원아이콘">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 208 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

이미지 크기는 가로 <?php echo $config['cf\_member\_img\_width'] ?>픽셀, 세로 <?php echo $config['cf\_member\_img\_height'] ?>픽셀 이하로 해주세요.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 209 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

gif, jpg, png파일만 가능하며 용량 <?php echo number\_format($config['cf\_member\_img\_size']) ?>바이트 이하만 등록됩니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 212 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<img src="<?php echo $mb\_img\_url ?>" alt="회원아이콘">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 220 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="mb\_mailling" value="1" id="reg\_mb\_mailling" <?php echo ($w=='' || $member['mb\_mailling'])?'checked':''; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 230 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="mb\_sms" value="1" id="reg\_mb\_sms" <?php echo ($w=='' || $member['mb\_sms'])?'checked':''; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 241 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="mb\_open" value="1" id="reg\_mb\_open" <?php echo ($w=='' || $member['mb\_open'])?'checked':''; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 248 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

정보공개를 바꾸시면 앞으로 <?php echo (int)$config['cf\_open\_modify'] ?>일 이내에는 변경이 안됩니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 250 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_open\_default" value="<?php echo $member['mb\_open'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 255 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_open" value="<?php echo $member['mb\_open'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 258 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

정보공개는 수정후 <?php echo (int)$config['cf\_open\_modify'] ?>일 이내, <?php echo date("Y년 m월 j일", isset($member['mb\_open\_date']) ? strtotime("{$member['mb\_open\_date']} 00:00:00")+$config['cf\_open\_modify']\*86400:G5\_SERVER\_TIME+$config['cf\_open\_modify']\*86400); ?> 까지는 변경이 안됩니다.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 287 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="submit" id="btn\_submit" class="btn\_submit" accesskey="s"><?php echo $w==''?'회원가입':'정보수정'; ?></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 349 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

certify\_win\_open("<?php echo $cert\_type; ?>", "<?php echo $cert\_url; ?>"+params);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form\_update.tail.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$receive\_number = preg\_replace("/[^0-9]/", "", $mb\_hp);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_form\_update.tail.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace("/[^0-9]/", "", $default['de\_admin\_company\_tel']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo get\_text($mb['mb\_name']); ?></strong>님의 회원가입을 진심으로 축하합니다.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $mb['mb\_id'] ?></strong><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\register\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $mb['mb\_email'] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['opener\_href\_wr\_id'] ?>" target="\_blank" class="scrap\_tit" onclick="opener.document.location.href='<?php echo $list[$i]['opener\_href\_wr\_id'] ?>'; return false;"><?php echo $list[$i]['subject'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['opener\_href'] ?>" class="scrap\_cate" target="\_blank" onclick="opener.document.location.href='<?php echo $list[$i]['opener\_href'] ?>'; return false;"><?php echo $list[$i]['bo\_subject'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="scrap\_datetime"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$i]['ms\_datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['del\_href']; ?>" onclick="del(this.href); return false;" class="scrap\_del"><i class="fa fa-trash-o" aria-hidden="true"></i><span class="sound\_only">삭제</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($i == 0) echo "<li class=\"empty\_list\">자료가 없습니다.</li>"; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($config['cf\_mobile\_pages'], $page, $total\_page, "?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\scrap\_popin.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\scrap\_popin.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\member\basic\scrap\_popin.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_text(cut\_str($write['wr\_subject'], 255)) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $group\_select ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_id" value="<?php echo $mb\_id ?>" id="mb\_id" placeholder="검색어를 입력하세요" required class="frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.getElementById("gr\_id").value = "<?php echo $gr\_id ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.getElementById("view").value = "<?php echo $view ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($list[$i]['bo\_table']); ?>" class="new\_board"><?php echo $bo\_subject ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['href'] ?>" class="new\_tit"><?php echo $list[$i]['comment'] ?><?php echo $wr\_subject ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자</span><?php echo $list[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="new\_date"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$i]['datetime2'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($member['mb\_id']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $nick ?>님</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == 'super' || $is\_auth) { ?><a href="<?php echo G5\_ADMIN\_URL ?>" class="btn\_admin"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $memo\_not\_read ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $point ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($member['mb\_id'], 60, 60); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="nickname"><?php echo $nick ?>님</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_BBS\_URL ?>/point.php" target="\_blank" class="point win\_point"><strong><?php echo $point ?></strong> 포인트

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == 'super' || $is\_auth) { ?><a href="<?php echo G5\_ADMIN\_URL ?>" class="btn\_admin">관리자</a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $memo\_not\_read; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo G5\_SHOP\_URL ?>/coupon.php" target="\_blank" class="win\_coupon"><i class="fa fa-ticket" aria-hidden="true"></i>쿠폰<strong><?php echo number\_format(get\_shop\_member\_coupon\_count($member['mb\_id'], true)); ?></strong></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="po\_id" value="<?php echo $po\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == "super") { ?><a href="<?php echo G5\_ADMIN\_URL ?>/poll\_form.php?w=u&amp;po\_id=<?php echo $po\_id ?>" class="btn\_admin btn"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자 관리</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo $po['po\_subject'] ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="gb\_poll" value="<?php echo $i ?>" id="gb\_poll\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="gb\_poll\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $po['po\_poll'.$i] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo " alert('권한 {$po['po\_level']} 이상의 회원만 투표에 참여하실 수 있습니다.'); return false; ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo " alert('권한 {$po['po\_level']} 이상의 회원만 결과를 보실 수 있습니다.'); return false; ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_all">전체 <?php echo $nf\_total\_po\_cnt ?>표</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $po\_subject ?> 결과</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php echo $poll\_1st\_class; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $list[$i]['content'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span style="width:<?php echo number\_format($list[$i]['rate'], 1) ?>%"></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="poll\_cnt"><?php echo $list[$i]['cnt'] ?> 표</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_percent"><?php echo number\_format($list[$i]['rate'], 1) ?> %</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $list2[$i]['pc\_name'] ?><span class="sound\_only">님의 의견</span></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list2[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_datetime"><?php echo $list2[$i]['datetime'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_cmt\_del"><?php if ($list2[$i]['del']) { echo $list2[$i]['del']."<i class=\"fa fa-times-circle\" aria-hidden=\"true\"></i><span class=\"sound\_only\">삭제</span></a>"; } ?></span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list2[$i]['idea'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="po\_id" value="<?php echo $po\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_member) { ?><input type="hidden" name="pc\_name" value="<?php echo get\_text(cut\_str($member['mb\_nick'],255)) ?>"><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h3><span>기타의견</span><?php echo $po\_etc ?></h3>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_guest) { echo chk\_captcha\_js(); } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo get\_text($token); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($admin\_href) { ?><li><a href="<?php echo $admin\_href ?>" class="btn\_admin btn"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="fix\_btn"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">문의등록</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $qaconfig['qa\_title'] ?> 카테고리</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="bo\_li<?php if ($is\_checkbox) echo ' bo\_adm'; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_qa\_id[]" value="<?php echo $list[$i]['qa\_id'] ?>" id="chk\_qa\_id\_<?php echo $i ?>" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_qa\_id\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<b class="sound\_only"><?php echo $list[$i]['subject'] ?></b>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="bo\_cate\_link"><?php echo $list[$i]['category']; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['view\_href']; ?>" class="bo\_subject">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['subject']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['icon\_file']) echo " <i class=\"fa fa-download\" aria-hidden=\"true\"></i>" ; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자</span><span><?php echo $list[$i]['name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_date"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$i]['date']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="li\_stat <?php echo ($list[$i]['qa\_status'] ? 'txt\_done' : 'txt\_rdy'); ?>"><?php echo ($list[$i]['qa\_status'] ? '답변완료' : '답변대기'); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($i == 0) { echo '<li class="empty\_list">게시물이 없습니다.</li>'; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list\_pages; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>전체 <?php echo number\_format($total\_count) ?>건</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $page ?> 페이지

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_qa\_sfl\_select\_options($sfl); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo stripslashes($stx) ?>" required placeholder="검색어를 입력하세요" id="stx" class="sch\_input" size="15" maxlength="15">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="tit\_cnt"><?php echo get\_text($answer['qa\_subject']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $answer['qa\_datetime']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_view\_thumbnail(conv\_content($answer['qa\_content'], $answer['qa\_html']), $qaconfig['qa\_image\_width']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $answer\_update\_href; ?>">답변수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $answer\_delete\_href; ?>" onclick="del(this.href); return false;">답변삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $rewrite\_href; ?>" class="add\_qu">추가질문</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qa\_id" value="<?php echo $view['qa\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo $token ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_hidden;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $option; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $list\_href ?>" class="btn\_b03 btn"><i class="fa fa-list" aria-hidden="true"></i><span class="sound\_only">목록</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $write\_href ?>" class="btn\_b03 btn"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($update\_href) { ?><li><a href="<?php echo $update\_href ?>"><i class="fa fa-pencil-square-o" aria-hidden="true"></i> 수정</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($delete\_href) { ?><li><a href="<?php echo $delete\_href ?>" onclick="del(this.href); return false;"><i class="fa fa-trash-o" aria-hidden="true"></i> 삭제</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_cate"><?php echo $view['category'] ;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_tit"><?php echo $view['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자</span><strong><?php echo $view['name'] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성일</span><strong><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $view['datetime']; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo $view['email']; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo $view['hp']; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_view\_thumbnail($view['img\_file'][$i], $qaconfig['qa\_image\_width']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="bo\_v\_con"><?php echo get\_view\_thumbnail($view['content'], $qaconfig['qa\_image\_width']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div><a href="<?php echo $rewrite\_href; ?>" class="btn\_b01">추가질문</a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['download\_href'][$i]; ?>" class="view\_file\_download" download>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<img src="<?php echo $qa\_skin\_url ?>/img/icon\_file.gif" alt="첨부">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $view['download\_source'][$i] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($prev\_href) { ?><li class="bo\_v\_prev"><a href="<?php echo $prev\_href ?>"><i class="fa fa-chevron-up" aria-hidden="true"></i><span class="sound\_only">이전글</span> <?php echo $prev\_qa\_subject;?></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($next\_href) { ?><li class="bo\_v\_next"><a href="<?php echo $next\_href ?>"><i class="fa fa-chevron-down" aria-hidden="true"></i><span class="sound\_only">다음글</span> <?php echo $next\_qa\_subject;?></a></li><?php } ?>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($qa\_skin\_path.'/view.answer.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($qa\_skin\_path.'/view.answerform.skin.php');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo get\_text($rel\_list[$i]['category']); ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $rel\_list[$i]['view\_href']; ?>" class="li\_sbj">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $rel\_list[$i]['subject']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="li\_stat <?php echo ($rel\_list[$i]['qa\_status'] ? 'txt\_done' : 'txt\_rdy'); ?>"><?php echo ($rel\_list[$i]['qa\_status'] ? '답변완료' : '답변대기'); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="li\_date"><?php echo $rel\_list[$i]['date']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fwrite" id="fwrite" action="<?php echo $action\_url ?>" onsubmit="return fwrite\_submit(this);" method="post" enctype="multipart/form-data" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qa\_id" value="<?php echo $qa\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo $token ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_hidden;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $option; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="email" name="qa\_email" value="<?php echo get\_text($write['qa\_email']); ?>" id="qa\_email" <?php echo $req\_email; ?> class="<?php echo $req\_email.' '; ?>frm\_input full\_input email" maxlength="100" placeholder="이메일">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qa\_email\_recv" value="1" id="qa\_email\_recv" <?php if($write['qa\_email\_recv']) echo 'checked="checked"'; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_hp" value="<?php echo get\_text($write['qa\_hp']); ?>" id="qa\_hp" <?php echo $req\_hp; ?> class="<?php echo $req\_hp.' '; ?>frm\_input full\_input" size="30" placeholder="휴대폰">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qa\_sms\_recv" value="1" id="qa\_sms\_recv" <?php if($write['qa\_sms\_recv']) echo 'checked="checked"'; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_subject" value="<?php echo get\_text($write['qa\_subject']); ?>" id="qa\_subject" required class="frm\_input full\_input required" maxlength="255" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="file" name="bf\_file[1]" id="bf\_file[1]" title="파일첨부 1 : 용량 <?php echo $upload\_max\_filesize; ?> 이하만 업로드 가능" class="frm\_file uploadBtn">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bf\_file\_del1"><?php echo $write['qa\_source1']; ?> 파일 삭제</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="file" name="bf\_file[2]" id="bf\_file[2]" title="파일첨부 2 : 용량 <?php echo $upload\_max\_filesize; ?> 이하만 업로드 가능" class="frm\_file uploadBtn">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bf\_file\_del2"><?php echo $write['qa\_source2']; ?> 파일 삭제</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list\_href; ?>" class="btn\_cancel">취소</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li>게시판<strong><?php echo $board\_count ?>개</strong></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li>게시물<strong><?php echo number\_format($total\_count) ?>개</strong></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><?php echo number\_format($page) ?>/<?php echo number\_format($total\_page) ?> 페이지 열람 중</li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="srows" value="<?php echo $srows ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $group\_select ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<script>document.getElementById("gr\_id").value = "<?php echo $gr\_id ?>";</script>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="wr\_subject||wr\_content"<?php echo get\_selected($sfl, "wr\_subject||wr\_content") ?>>제목+내용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="wr\_subject"<?php echo get\_selected($sfl, "wr\_subject") ?>>제목</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="wr\_content"<?php echo get\_selected($sfl, "wr\_content") ?>>내용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mb\_id"<?php echo get\_selected($sfl, "mb\_id") ?>>회원아이디</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="wr\_name"<?php echo get\_selected($sfl, "wr\_name") ?>>이름</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" id="stx" value="<?php echo $text\_stx ?>" class="frm\_input" required maxlength="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" value="or" <?php echo ($sop == "or") ? "checked" : ""; ?> id="sop\_or" name="sop">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" value="and" <?php echo ($sop == "and") ? "checked" : ""; ?> id="sop\_and" name="sop">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="?<?php echo $search\_query ?>&amp;gr\_id=<?php echo $gr\_id ?>" <?php echo $sch\_all ?>>전체게시판</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str\_board\_list; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><a href="<?php echo get\_pretty\_url($search\_table[$idx], '', $search\_query); ?>"><?php echo $bo\_subject[$idx] ?> 게시판 내 결과</a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$idx][$i]['href'] ?><?php echo $comment\_href ?>"><?php echo $comment\_def ?><?php echo $list[$idx][$i]['subject'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <a href="<?php echo $list[$idx][$i]['href'] ?><?php echo $comment\_href ?>" target="\_blank" class="sch\_res\_new"><i class="fa fa-share-square-o" aria-hidden="true"></i><span class="sound\_only">새창</span></a> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo $list[$idx][$i]['content'] ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$idx][$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sch\_datetime"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$idx][$i]['wr\_datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sch\_more"><a href="<?php echo get\_pretty\_url($search\_table[$idx], '', $search\_query); ?>"><strong><?php echo $bo\_subject[$idx] ?></strong> 결과 더보기</a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\boxbanner.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i==0) echo '<aside id="sbn\_side"><h2>쇼핑몰 배너</h2><ul class="sb\_bn">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\boxbanner.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $banner.'<img src="'.G5\_DATA\_URL.'/banner/'.$row['bn\_id'].'" alt="'.get\_text($row['bn\_alt']).'" width="'.$size[0].'" height="'.$size[1].'"'.$bn\_border.'>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\boxbanner.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i>0) echo '</ul></aside>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($tv\_tot\_count == 0) echo '<ul id="stv\_ul">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li class="stv\_item c'.$k.'">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $img;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($tv\_tot\_count > 0) echo '</ul>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var itemQty = <?php echo $tv\_tot\_count; ?>;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var itemShow = <?php echo $tv\_div['img\_length']; ?>;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var EOFlag = parseInt(<?php echo $i-1; ?>/itemShow);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var itemRest = parseInt(<?php echo $i-1; ?>%itemShow);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\couponzone.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo $default['de\_admin\_company\_name']; ?> 회원이시라면 쿠폰 다운로드 후 바로 사용하실 수 있습니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\couponzone.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<ul>'.PHP\_EOL.$coupon.'</ul>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\couponzone.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p>보유하신 <?php echo $default['de\_admin\_company\_name']; ?> 회원 포인트를 쿠폰으로 교환하실 수 있습니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 181 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\couponzone.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<ul>'.PHP\_EOL.$coupon.'</ul>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

Kakao.init("<?php echo $config['cf\_kakao\_js\_apikey']; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fitem" action="<?php echo $action\_url; ?>" method="post" onsubmit="return fitem\_submit(this);">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[]" value="<?php echo $it['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $thumb\_img;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong id="sit\_title"><?php echo stripslashes($it['it\_name']); ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($it['it\_basic']) { ?><p id="sit\_desc"><?php echo $it['it\_basic']; ?></p><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p id="sit\_opt\_info">상품 선택옵션 <?php echo $option\_count; ?> 개, 추가옵션 <?php echo $supply\_count; ?> 개</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">고객평점 <?php echo $score?>개</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<img src="<?php echo G5\_SHOP\_URL; ?>/img/s\_star<?php echo $score?>.png" alt="" class="sit\_star" width="100">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="review\_num">사용후기 <?php echo $it['it\_use\_cnt']; ?> 개</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="btn\_wish"><i class="fa fa-heart-o" aria-hidden="true"></i><span class="sound\_only">위시리스트</span><span class="btn\_wish\_num"><?php echo get\_wishlist\_count\_by\_item($it['it\_id']); ?></span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/facebook.png'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/twitter.png'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/gplus.png'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_sns\_share\_link('kakaotalk', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/sns\_kakao.png'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:popup\_item\_recommend('<?php echo $it['it\_id']; ?>');" id="sit\_btn\_rec"><i class="fa fa-envelope-o" aria-hidden="true"></i><span class="sound\_only">추천하기</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $it['it\_maker']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $it['it\_origin']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $it['it\_brand']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $it['it\_model']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_price($it['it\_cust\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo display\_price(get\_price($it)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="it\_price" value="<?php echo get\_price($it); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 174 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '구매금액(추가옵션 제외)의 '.$it['it\_point'].'%';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo number\_format($it\_point).'점';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 203 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th><?php echo $ct\_send\_cost\_label; ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 204 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $sc\_method; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 209 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($it['it\_buy\_min\_qty']); ?> 개</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 215 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($it['it\_buy\_max\_qty']); ?> 개</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 230 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $prev\_href.$prev\_title.$prev\_href2;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 231 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $next\_href.$next\_title.$next\_href2;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_SHOP\_URL; ?>/largeimage.php?it\_id=<?php echo $it['it\_id']; ?>&amp;no=1" target="\_blank" class="popup\_item\_image "><i class="fa fa-search-plus" aria-hidden="true"></i><span class="sound\_only">확대보기</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 255 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_item;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 271 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $supply\_item;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 288 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_type[<?php echo $it\_id; ?>][]" value="0">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 289 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_id[<?php echo $it\_id; ?>][]" value="">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 290 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_value[<?php echo $it\_id; ?>][]" value="<?php echo $it['it\_name']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 292 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" class="io\_stock" value="<?php echo $it['it\_stock\_qty']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 294 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sit\_opt\_subj"><?php echo $it['it\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 297 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ct\_qty\_<?php echo $i; ?>" class="sound\_only">수량</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 299 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ct\_qty[<?php echo $it\_id; ?>][]" value="<?php echo $it['it\_buy\_min\_qty']; ?>" id="ct\_qty\_<?php echo $i; ?>" class="num\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 325 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:popup\_stocksms('<?php echo $it['it\_id']; ?>');" id="sit\_btn\_phone">재입고알림</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 327 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:item\_wish(document.fitem, '<?php echo $it['it\_id']; ?>');" id="sit\_btn\_wish"><span class="sound\_only">위시리스트</span><i class="fa fa-heart-o" aria-hidden="true"></i></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 329 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="naverpay-item"><?php echo $naverpay\_request\_js.$naverpay\_button\_js; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 363 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo ($it['it\_mobile\_explan'] ? conv\_content($it['it\_mobile\_explan'], 1) : conv\_content($it['it\_explan'], 1)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 383 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><?php echo $ii\_title; ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 384 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $ii\_value; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 421 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($default['de\_baesong\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 431 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($default['de\_change\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 465 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 573 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var min\_qty = parseInt(<?php echo $it['it\_buy\_min\_qty']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 574 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var max\_qty = parseInt(<?php echo $it['it\_buy\_max\_qty']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 623 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

f.action = "<?php echo $action\_url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 645 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var min\_qty = parseInt(<?php echo $it['it\_buy\_min\_qty']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 646 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var max\_qty = parseInt(<?php echo $it['it\_buy\_max\_qty']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\iteminfo.change.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($default['de\_change\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\iteminfo.delivery.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($default['de\_baesong\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\iteminfo.delivery.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($default['de\_change\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\iteminfo.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $it['it\_basic']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\iteminfo.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo ($it['it\_mobile\_explan'] ? conv\_content($it['it\_mobile\_explan'], 1) : conv\_content($it['it\_explan'], 1)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\iteminfo.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $ii\_title; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\iteminfo.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $ii\_value; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\iteminfo.relation.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemqa\_form; ?>" class="itemqa\_form qa\_wr">상품문의 쓰기<span class="sound\_only"> 새 창</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemqa\_list; ?>" id="itemqa\_list" class="btn01">더보기</a>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqa.skin.php

MD5 Hashing algorithm.

$hash = md5($row['iq\_id'].$row['iq\_time'].$row['iq\_ip']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<ol id="sit\_qa\_ol">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" class="sit\_qa\_li\_title"><?php echo $iq\_subject; ?></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo $iq\_name; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $iq\_time; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="<?php echo $iq\_style; ?>"><?php echo $iq\_stats; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sit\_qa\_con\_<?php echo $i; ?>" class="sit\_qa\_con">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $iq\_question;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $iq\_answer; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemqa\_form."&amp;iq\_id={$row['iq\_id']}&amp;w=u"; ?>" class="itemqa\_form btn01" onclick="return false;">수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemqa\_formupdate."&amp;iq\_id={$row['iq\_id']}&amp;w=d&amp;hash={$hash}"; ?>" class="itemqa\_delete btn01">삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo '</ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (!$i) echo '<p class="sit\_empty">상품문의가 없습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo itemqa\_page($config['cf\_mobile\_pages'], $page, $total\_page, G5\_SHOP\_URL."/itemqa.php?it\_id=$it\_id&amp;page=", "");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id" value="<?php echo $it\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="iq\_id" value="<?php echo $iq\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="iq\_secret" id="iq\_secret" value="1" <?php echo $chk\_secret; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="email" name="iq\_email" id="iq\_email" value="<?php echo get\_text($qa['iq\_email']); ?>" class="frm\_input full\_input" size="30" placeholder="이메일"> <span class="frm\_info ">이메일을 입력하시면 답변 등록 시 답변이 이메일로 전송됩니다.</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="iq\_hp" id="iq\_hp" value="<?php echo get\_text($qa['iq\_hp']); ?>" class="frm\_input full\_input" size="20" placeholder="휴대폰"> <span class="frm\_info ">휴대폰번호를 입력하시면 답변 등록 시 답변등록 알림이 SMS로 전송됩니다.</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="iq\_subject" value="<?php echo get\_text($qa['iq\_subject']); ?>" id="iq\_subject" required class="required frm\_input full\_input" minlength="2" maxlength="250" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form method="get" action="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="b.it\_name" <?php echo get\_selected($sfl, "b.it\_name", true); ?>>상품명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.it\_id" <?php echo get\_selected($sfl, "a.it\_id"); ?>>상품코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.iq\_subject" <?php echo get\_selected($sfl, "a.iq\_subject"); ?>>문의제목</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.iq\_question"<?php echo get\_selected($sfl, "a.iq\_question"); ?>>문의내용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.iq\_name" <?php echo get\_selected($sfl, "a.it\_id"); ?>>작성자명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.mb\_id" <?php echo get\_selected($sfl, "a.mb\_id"); ?>>작성자아이디</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx; ?>" id="stx" required class="sch\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">전체보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <p><?php echo $config['cf\_title']; ?> 전체 상품문의 목록입니다.</p> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $it\_href; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_it\_image($row['it\_id'], 60, 60); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $row['it\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><span class="<?php echo $iq\_style; ?>"><?php echo $iq\_stats; ?></span> <?php echo $iq\_subject; ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sqa\_if\_wt"><?php echo get\_text($row['iq\_name']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo substr($row['iq\_time'],2,8); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sqa\_con\_<?php echo $i; ?>" class="sqa\_con" style="display:none;">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $iq\_question;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $iq\_answer; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sqa\_con\_btn"><button class="sqa\_con\_<?php echo $i; ?>"><span class="sound\_only">내용보기</span><i class="fa fa-chevron-down" aria-hidden="true"></i></button></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo '</ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<p id="sps\_empty">자료가 없습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($config['cf\_mobile\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemuse\_form; ?>" class="qa\_wr itemuse\_form " onclick="return false;">사용후기 쓰기<span class="sound\_only"> 새 창</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemuse\_list; ?>" id="itemuse\_list" class="btn01">더보기</a>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuse.skin.php

MD5 Hashing algorithm.

$hash = md5($row['is\_id'].$row['is\_time'].$row['is\_ip']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<ol id="sit\_use\_ol">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" class="sit\_use\_li\_title"><?php echo $is\_subject; ?></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo $is\_name; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $is\_time; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sit\_use\_star"><img src="<?php echo G5\_SHOP\_URL; ?>/img/s\_star<?php echo $is\_star; ?>.png" alt="별<?php echo $is\_star; ?>개"></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sit\_use\_con\_<?php echo $i; ?>" class="sit\_use\_con">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemuse\_form."&amp;is\_id={$row['is\_id']}&amp;w=u"; ?>" class="itemuse\_form btn01" onclick="return false;">수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemuse\_formupdate."&amp;is\_id={$row['is\_id']}&amp;w=d&amp;hash={$hash}"; ?>" class="itemuse\_delete btn01">삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_reply\_subject;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_reply\_name;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_reply\_content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo '</ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (!$i) echo '<p class="sit\_empty">사용후기가 없습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo itemuse\_page($config['cf\_mobile\_pages'], $page, $total\_page, G5\_SHOP\_URL."/itemuse.php?it\_id=$it\_id&amp;page=", "");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id" value="<?php echo $it\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="is\_id" value="<?php echo $is\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="is\_subject" value="<?php echo get\_text($use['is\_subject']); ?>" id="is\_subject" required class="required frm\_input" minlength="2" maxlength="250" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="5" id="is\_score10" <?php echo ($is\_score==5)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="4" id="is\_score8" <?php echo ($is\_score==4)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="3" id="is\_score6" <?php echo ($is\_score==3)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="2" id="is\_score4" <?php echo ($is\_score==2)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="1" id="is\_score2" <?php echo ($is\_score==1)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form method="get" action="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="b.it\_name" <?php echo get\_selected($sfl, "b.it\_name"); ?>>상품명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.it\_id" <?php echo get\_selected($sfl, "a.it\_id"); ?>>상품코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.is\_subject"<?php echo get\_selected($sfl, "a.is\_subject"); ?>>후기제목</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.is\_content"<?php echo get\_selected($sfl, "a.is\_content"); ?>>후기내용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.is\_name" <?php echo get\_selected($sfl, "a.is\_name"); ?>>작성자명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.mb\_id" <?php echo get\_selected($sfl, "a.mb\_id"); ?>>작성자아이디</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx; ?>" id="stx" required class="sch\_input" size="10">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">전체보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <p><?php echo $config['cf\_title']; ?> 전체 사용후기 목록입니다.</p> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $it\_href; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_itemuselist\_thumbnail($row['it\_id'], $row['is\_content'], 70, 70); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $row2['it\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">평가점수</span><img src="<?php echo G5\_SHOP\_URL; ?>/img/s\_star<?php echo $star; ?>.png" alt="별<?php echo $star; ?>개" width="80">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button class="sps\_con\_<?php echo $i; ?> review\_detail"><?php echo get\_text($row['is\_subject']); ?></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo get\_text($row['is\_subject']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sps\_dd\_wt"><?php echo $row['is\_name']; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo substr($row['is\_time'],0,10); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_itemuselist\_thumbnail($row['it\_id'], $row['is\_content'], 50, 50); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo get\_text($row['is\_subject']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">평가점수</span><img src="<?php echo G5\_URL; ?>/shop/img/s\_star<?php echo $star; ?>.png" alt="별<?php echo $star; ?>개" width="80">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sps\_con\_<?php echo $i; ?>" class="review\_bt\_cnt">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="is\_use\_reply"><?php echo get\_text($row['is\_reply\_subject']); ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $row['is\_reply\_name']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sps\_con\_<?php echo $i; ?>\_reply">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_reply\_content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sps\_if\_wt"><?php echo get\_text($row['is\_name']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo substr($row['is\_time'],2,8); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo '</ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<p id="sps\_empty">자료가 없습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($config['cf\_mobile\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\largeimage.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<img src="<?php echo $imageurl; ?>" width="<?php echo $size[0]; ?>" alt="<?php echo $row['it\_name']; ?>" id="largeimage\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\largeimage.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><a href="'.G5\_SHOP\_URL.'/largeimage.php?it\_id='.$it\_id.'&amp;no='.$key.'" class="img\_thumb">'.$val.'</a></li>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\largeimage.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$("#sit\_pvi\_nwbig span:eq("+<?php echo ($no - 1); ?>+")").addClass("visible");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

Kakao.init("<?php echo $config['cf\_kakao\_js\_apikey']; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul id=\"sct\_wrap\" class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul id=\"sct\_wrap\" class=\"sct ".$ul\_sct\_class."\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$li\_clear}\"$li\_width\_style><div class=\"li\_wr is\_view\_type\_list\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_star\"><span class=\"sound\_only\">고객평점</span><img src=\"".G5\_SHOP\_URL."/img/s\_star".$star\_score.".png\" alt=\"별점 ".$star\_score."점\" class=\"sit\_star\"></div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_basic\">".stripslashes($row['it\_basic'])."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<button type=\"button\" class=\"btn\_wish\" data-it\_id=\"{$row['it\_id']}\"><span class=\"sound\_only\">위시리스트</span><i class=\"fa fa-heart-o\" aria-hidden=\"true\"></i></button>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/facebook.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/twitter.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/gplus.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('kakaotalk', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/sns\_kakao.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_icon\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var li\_width = "<?php echo intval(100 / $this->list\_mod); ?>",

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

img\_width = "<?php echo $this->img\_width; ?>",

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

img\_height = "<?php echo $this->img\_height; ?>",

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

list\_ca\_id = "<?php echo $this->ca\_id; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.best.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li class="sct\_li"'.$li\_width\_style.'>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.best.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="sct\_img"><a href="'.$this->href.$row['it\_id'].'" class="sct\_a">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.best.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name'])).PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.best.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="sct\_id">&lt;'.stripslashes($row['it\_id']).'&gt;</div>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.best.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="sct\_txt"><a href="'.$this->href.$row['it\_id'].'" class="sct\_a">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.best.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name']).PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.best.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="sct\_cost">'.display\_price(get\_price($row), $row['it\_tel\_inq']).'</div>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.best.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="bst\_silde\_btn">'.$slide\_btn.'</div>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_price&amp;sortodr=asc" >낮은가격순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_price&amp;sortodr=desc">높은가격순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_name&amp;sortodr=asc">상품명순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\listcategory.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

Kakao.init("<?php echo $config['cf\_kakao\_js\_apikey']; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$li\_clear}\"$li\_width\_style><div class=\"li\_wr is\_view\_type\_list\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_star\"><img src=\"".G5\_SHOP\_URL."/img/s\_star".$star\_score.".png\" alt=\"별점 ".$star\_score."점\" class=\"sit\_star\"></div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$this->href}{$row['it\_id']}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_basic\">".stripslashes($row['it\_basic'])."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<button type=\"button\" class=\"btn\_wish\" data-it\_id=\"{$row['it\_id']}\"><span class=\"sound\_only\">위시리스트</span><i class=\"fa fa-heart-o\" aria-hidden=\"true\"></i></button>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/facebook.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/twitter.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/gplus.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('kakaotalk', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/sns\_kakao.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_icon\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

Kakao.init("<?php echo $config['cf\_kakao\_js\_apikey']; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$li\_clear}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"li\_wr\" style=\"padding-left:{$this->img\_width}px;height:{$this->img\_height}px\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_star\"><img src=\"".G5\_SHOP\_URL."/img/s\_star".$star\_score.".png\" alt=\"별점 ".$star\_score."점\" class=\"sit\_star\"></div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$this->href}{$row['it\_id']}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_icon\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_sns\" style=\"top:{$sns\_top}px\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/facebook.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/twitter.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/gplus.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('kakaotalk', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/sns\_kakao.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

Kakao.init("<?php echo $config['cf\_kakao\_js\_apikey']; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$li\_clear}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_star\"><img src=\"".G5\_SHOP\_URL."/img/s\_star".$star\_score.".png\" alt=\"별점 ".$star\_score."점\" class=\"sit\_star\"></div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$this->href}{$row['it\_id']}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_sns\" style=\"top:{$sns\_top}px\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/facebook.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/twitter.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/gplus.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('kakaotalk', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/sns\_kakao.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.event.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="'.$href.'" class="sev\_img"><img src="'.G5\_DATA\_URL.'/event/'.$row['ev\_id'].'\_m" alt="'.$row['ev\_subject'].'"></a>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.event.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="'.$href.'" class="sev\_text">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.event.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($row['ev\_subject\_strong']) echo '<strong>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.event.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $row['ev\_subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.event.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($row['ev\_subject\_strong']) echo '</strong>';

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.event.skin.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

from `{$g5['g5\_shop\_event\_item\_table']}` a left join `{$g5['g5\_shop\_item\_table']}` b on (a.it\_id = b.it\_id)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.event.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li class="ev\_prd\_'.$k.'">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\main.event.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<span class="ev\_prd\_img">'.get\_it\_image($row2['it\_id'], 300, 300, get\_text($row2['it\_name'])).'</span>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\mainbanner.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i==0) echo '<div id="main\_bn"><div class="main\_banner\_owl owl-carousel">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\mainbanner.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $banner.'<img src="'.G5\_DATA\_URL.'/banner/'.$row['bn\_id'].'" width="'.$size[0].'" alt="'.get\_text($row['bn\_alt']).'"'.$bn\_border.'>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\navigation.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="sct\_li<?php echo $li\_clear; ?>"<?php echo $li\_width\_style; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sct\_img"><a href="<?php echo $href; ?>" class="sct\_a"><img src="<?php echo G5\_MSHOP\_SKIN\_URL; ?>/img/personal.jpg" alt=""></a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sct\_txt"><a href="<?php echo $href; ?>" class="sct\_a"><?php echo get\_text($row['pp\_name']).'님 개인결제'; ?></a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sct\_cost"><?php echo display\_price($row['pp\_price']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 개인결제가 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

Kakao.init("<?php echo $config['cf\_kakao\_js\_apikey']; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul id=\"sct\_wrap\" class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$li\_clear}\"$li\_width\_style><div class=\"li\_wr\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$this->href}{$row['it\_id']}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"{$this->href}{$row['it\_id']}\" class=\"sct\_txt\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 관련상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

검색 결과 <b><?php echo $total\_count; ?></b>건

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qsort" id="qsort" value="<?php echo $qsort ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qorder" id="qorder" value="<?php echo $qorder ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qcaid" id="qcaid" value="<?php echo $qcaid ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="q" value="<?php echo $q; ?>" id="ssch\_q" class="frm\_input" maxlength="30">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qname" id="ssch\_qname" <?php echo $qname\_check?'checked="checked"':'';?> class="selec\_chk"> <label for="ssch\_qname"><span></span>상품명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qexplan" id="ssch\_qexplan" <?php echo $qexplan\_check?'checked="checked"':'';?> class="selec\_chk"> <label for="ssch\_qexplan"><span></span> <span class="sound\_only">상품</span>설명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qbasic" id="ssch\_qbasic" value="1" <?php echo $qbasic\_check?'checked="checked"':'';?> class="selec\_chk"> <label for="ssch\_qbasic"><span></span> 기본설명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qid" id="ssch\_qid" <?php echo $qid\_check?'checked="checked"':'';?> class="selec\_chk"> <label for="ssch\_qid"><span></span><span class="sound\_only"> 상품</span>코드</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qfrom" value="<?php echo $qfrom; ?>" id="ssch\_qfrom" class="frm\_input" size="6"> 원 ~

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qto" value="<?php echo $qto; ?>" id="ssch\_qto" class="frm\_input" size="6"> 원<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><a href="#" onclick="set\_ca\_id(\'\'); return false;">전체분류 <span>'.$total\_count.'</span></a></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li><a href=\"#\" onclick=\"set\_ca\_id('{$row['ca\_id']}'); return false;\">{$row['ca\_name']} <span>".$row['cnt']."</span></a></li>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div>'.$error.'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_paging($config['cf\_mobile\_pages'], $page, $total\_page, $\_SERVER['SCRIPT\_NAME'].'?'.$query\_string.'&amp;page=');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fregisterform" id="fregisterform" action="<?php echo $register\_action\_url; ?>" onsubmit="return fregisterform\_submit(this);" method="POST" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea readonly><?php echo get\_text($config['cf\_stipulation']) ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td>아이디, 이름, 비밀번호<?php echo ($config['cf\_cert\_use']) ? ", 생년월일, 휴대폰 번호(본인인증 할 때만, 아이핀 제외), 암호화된 개인식별부호(CI)" : ""; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="provider" value="<?php echo $provider\_name; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cert\_type" value="<?php echo $member['mb\_certify']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $user\_id; ?>" id="reg\_mb\_id">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="reg\_mb\_name" name="mb\_name" value="<?php echo $user\_name ? $user\_name : $user\_nick ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_hp" value="<?php echo get\_text($user\_phone); ?>" id="reg\_mb\_hp">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="old\_mb\_hp" value="<?php echo get\_text($user\_phone); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

닉네임을 바꾸시면 앞으로 <?php echo (int)$config['cf\_nick\_modify'] ?>일 이내에는 변경 할 수 없습니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_nick\_default" value="<?php echo isset($user\_nick) ? get\_text($user\_nick) : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_nick" value="<?php echo isset($user\_nick) ? get\_text($user\_nick) : ''; ?>" id="reg\_mb\_nick" required class="frm\_input required nospace full\_input" size="10" maxlength="20" placeholder="닉네임 (필수)">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($w=='') { echo "E-mail 로 발송된 내용을 확인한 후 인증하셔야 회원가입이 완료됩니다."; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($w=='u') { echo "E-mail 주소를 변경하시면 다시 인증하셔야 합니다."; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="old\_email" value="<?php echo $member['mb\_email'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_email" value="<?php echo isset($user\_email) ? $user\_email : ''; ?>" id="reg\_mb\_email" required <?php echo (isset($user\_email) && $user\_email != '' && !$is\_exists\_email)? "readonly":''; ?> class="frm\_input email full\_input required" size="70" maxlength="100" placeholder="E-mail (필수)">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="check"><?php echo $email\_msg; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="submit" id="btn\_submit" class="btn\_submit" accesskey="s"><?php echo $w == '' ? '회원가입' : '정보수정'; ?></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 174 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form method="post" action="<?php echo $login\_action\_url ?>" onsubmit="return social\_obj.flogin\_submit(this);">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 175 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="url" name="url" value="<?php echo $login\_url ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="provider" name="provider" value="<?php echo $provider\_name ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 267 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

certify\_win\_open("<?php echo $cert\_type; ?>", "<?php echo $cert\_url; ?>" + params);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_u\_register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $link\_href; ?>" id="sns-<?php echo $social; ?>" class="sns-icon social\_link sns-<?php echo $social; ?><?php echo $add\_class; ?>" title="<?php echo $title; ?>" data-provider="<?php echo $social; ?>" ><span class="ico"></span><span class="txt"><?php echo $provider\_name; ?> 로그인</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_u\_register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

socials["<?php echo $social; ?>"] = "<?php echo social\_nonce\_create($social, $session\_id); ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\social\social\_u\_register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

self\_url = "<?php echo $self\_url; ?>",

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo number\_format($visit[1]) ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo number\_format($visit[2]) ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo number\_format($visit[3]) ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo number\_format($visit[4]) ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\mobile\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == "super") { ?><a href="<?php echo G5\_ADMIN\_URL ?>/visit\_list.php" class="btn\_admin btn"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">상세보기</span></a></a><?php } ?>

**STANDARD: Potentially Unsafe Code - fopen**

Line: 550 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\browscap\Browscap.php

$lockRes = fopen($lockfile, 'w+');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 550 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\browscap\Browscap.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$lockRes = fopen($lockfile, 'w+');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 575 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\browscap\Browscap.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$iniContent = file\_get\_contents($ini\_path);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 584 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\browscap\Browscap.php

MD5 Hashing algorithm.

$tmpFile = $dir . '/temp\_' . md5(time() . basename($cache\_path));

**STANDARD: Potentially Unsafe Code - fopen**

Line: 587 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\browscap\Browscap.php

if (false === ($fileRes = fopen($tmpFile, 'w+'))) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 587 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\browscap\Browscap.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (false === ($fileRes = fopen($tmpFile, 'w+'))) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 592 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\browscap\Browscap.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (false === fwrite($fileRes, $this->\_buildCache())) {

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 672 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\browscap\Browscap.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$compressedPattern = preg\_replace(

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 787 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\browscap\Browscap.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$compressedPattern = preg\_replace(

**STANDARD: Potentially Unsafe Code - fopen**

Line: 1167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\browscap\Browscap.php

$test\_file = fopen($path, 'a');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\browscap\Browscap.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$test\_file = fopen($path, 'a');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1209 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\browscap\Browscap.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$content = preg\_replace('/<[?%].\*[?%]>/', '', $content);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1329 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\browscap\Browscap.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$file = file\_get\_contents($url);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1340 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\browscap\Browscap.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$file = file\_get\_contents($url, false, $context);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1384 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\browscap\Browscap.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($remote\_handler, $out);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1457 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\browscap\Browscap.php

nothing to do here

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\debugbar\debugbar.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo 'PHP 실행시간 : '.$php\_run\_time.' | 메모리 사용량 : '.number\_format($memory\_usage).' bytes'; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\debugbar\debugbar.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

총 쿼리수 : <span><?php echo isset($g5\_debug['sql']) ? count($g5\_debug['sql']) : 0; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\debugbar\debugbar.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td scope="row" data-label="실행순서"><?php echo $key; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\debugbar\debugbar.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="left" data-label="쿼리문"><?php echo $query['sql']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\debugbar\debugbar.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td data-label="실행시간"><?php echo $show\_excuted\_time.' ms'; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\debugbar\debugbar.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td scope="row" data-label="event\_tag" <?php echo $rowspan; ?>><?php echo $tag.' <span class="hook\_count">('.$count.')</span>'; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\debugbar\debugbar.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $print\_function; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\debugbar\debugbar.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td data-label="인수의 수"><?php echo $data['arguments']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\debugbar\debugbar.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td data-label="우선 순위"><?php echo $data['priority']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\debugbar\debugbar.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td scope="row" data-label="event\_tag"><?php echo $tag.' <span class="hook\_count">('.$count.')</span>'; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 234 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\debugbar\debugbar.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td scope="row" data-label="replace\_tag" <?php echo $rowspan; ?>><?php echo $tag.' <span class="hook\_count">('.$count.')</span>'; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 237 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\debugbar\debugbar.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $print\_function; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 239 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\debugbar\debugbar.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td data-label="인수의 수"><?php echo $data['arguments']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 240 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\debugbar\debugbar.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td data-label="우선 순위"><?php echo $data['priority']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 248 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\debugbar\debugbar.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td scope="row" data-label="replace\_tag"><?php echo $tag.' <span class="hook\_count">('.$count.')</span>'; ?></td>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\cheditor5\editor.lib.php

MD5 Hashing algorithm.

define( 'FT\_NONCE\_SESSION\_KEY' , substr(md5(FT\_NONCE\_UNIQUE\_KEY), 5) );

**MEDIUM: Potentially Unsafe Code - md5**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\cheditor5\editor.lib.php

MD5 Hashing algorithm.

return md5(FT\_NONCE\_UNIQUE\_KEY.$secret);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\cheditor5\imageUpload\config.php

MD5 Hashing algorithm.

$tmp\_name = md5(sha1($tmp\_name));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\cheditor5\imageUpload\delete.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$filesrc = isset($\_POST["filesrc"]) ? preg\_replace("/[ #\&\+\-%@=\/\\\:;,\'\"\^`~|\!\?\\*$#<>()\[\]\{\}]/", "", $\_POST["filesrc"]) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\cheditor5\imageUpload\delete.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $r ? true : false;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\cheditor5\imageUpload\upload.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $rdata;

**STANDARD: Potentially Unsafe Code - exec**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\editor.lib.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return "var {$id}\_editor\_data = oEditors.getById['{$id}'].getIR();\noEditors.getById['{$id}'].exec('UPDATE\_CONTENTS\_FIELD', []);\nif(jQuery.inArray(document.getElementById('{$id}').value.toLowerCase().replace(/^\s\*|\s\*$/g, ''), ['&nbsp;','<p>&nbsp;</p>','<p><br></p>','<div><br></div>','<p></p>','<br>','']) != -1){document.getElementById('{$id}').value='';}\n";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\editor.lib.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

return "var {$id}\_editor\_data = oEditors.getById['{$id}'].getIR();\noEditors.getById['{$id}'].exec('UPDATE\_CONTENTS\_FIELD', []);\nif(jQuery.inArray(document.getElementById('{$id}').value.toLowerCase().replace(/^\s\*|\s\*$/g, ''), ['&nbsp;','<p>&nbsp;</p>','<p><br></p>','<div><br></div>','<p></p>','<br>','']) != -1){document.getElementById('{$id}').value='';}\n";

**STANDARD: Potentially Unsafe Code - exec**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\editor.lib.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return "if (!{$id}\_editor\_data || jQuery.inArray({$id}\_editor\_data.toLowerCase(), ['&nbsp;','<p>&nbsp;</p>','<p><br></p>','<p></p>','<br>']) != -1) { alert(\"내용을 입력해 주십시오.\"); oEditors.getById['{$id}'].exec('FOCUS'); return false; }\n";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\editor.lib.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

return "if (!{$id}\_editor\_data || jQuery.inArray({$id}\_editor\_data.toLowerCase(), ['&nbsp;','<p>&nbsp;</p>','<p><br></p>','<p></p>','<br>']) != -1) { alert(\"내용을 입력해 주십시오.\"); oEditors.getById['{$id}'].exec('FOCUS'); return false; }\n";

**MEDIUM: Potentially Unsafe Code - md5**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\editor.lib.php

MD5 Hashing algorithm.

define( 'FT\_NONCE\_SESSION\_KEY' , substr(md5(FT\_NONCE\_UNIQUE\_KEY), 5) );

**MEDIUM: Potentially Unsafe Code - md5**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\editor.lib.php

MD5 Hashing algorithm.

return md5(FT\_NONCE\_UNIQUE\_KEY.$secret);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 553 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\photo\_uploader\popup\php\JSON.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace(array(

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 374 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\photo\_uploader\popup\php\UploadHandler.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$bytes = (int) preg\_replace('/[^0-9]/', '', $val);

**STANDARD: Potentially Unsafe Code - exec**

Line: 972 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\photo\_uploader\popup\php\UploadHandler.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

exec($cmd, $output, $error);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 972 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\photo\_uploader\popup\php\UploadHandler.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

exec($cmd, $output, $error);

**STANDARD: Potentially Unsafe Code - exec**

Line: 998 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\photo\_uploader\popup\php\UploadHandler.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

exec($cmd, $output, $error);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 998 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\photo\_uploader\popup\php\UploadHandler.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

exec($cmd, $output, $error);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 1073 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\photo\_uploader\popup\php\UploadHandler.php

MD5 Hashing algorithm.

$tmp\_name = md5(sha1($tmp\_name));

**STANDARD: Potentially Unsafe Code - fopen**

Line: 1156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\photo\_uploader\popup\php\UploadHandler.php

fopen($uploaded\_file, 'r'),

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\photo\_uploader\popup\php\UploadHandler.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fopen($uploaded\_file, 'r'),

**STANDARD: Potentially Unsafe Code - fopen**

Line: 1166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\photo\_uploader\popup\php\UploadHandler.php

fopen('php:

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1221 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\photo\_uploader\popup\php\UploadHandler.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

protected function readfile($file\_path) {

**STANDARD: Potentially Unsafe Code - fopen**

Line: 1225 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\photo\_uploader\popup\php\UploadHandler.php

$handle = fopen($file\_path, 'rb');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1225 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\photo\_uploader\popup\php\UploadHandler.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$handle = fopen($file\_path, 'rb');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1227 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\photo\_uploader\popup\php\UploadHandler.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo fread($handle, $chunk\_size);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1234 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\photo\_uploader\popup\php\UploadHandler.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

return readfile($file\_path);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1238 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\photo\_uploader\popup\php\UploadHandler.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $str;

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1351 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\photo\_uploader\popup\php\UploadHandler.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$this->readfile($file\_path);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1413 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\editor\smarteditor2\photo\_uploader\popup\php\UploadHandler.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

rawurldecode(preg\_replace(

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\extend.video.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace('#</iframe>#i', '</img>', $str);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

:TODO: make the config merge in, instead of replace

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 631 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace('/(rgba|hsla)\('.$p.','.$p.','.$p.','.$p.'\)/', '\1(\2,\5,\8,\11)', $string);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 634 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace('/(rgb|hsl)\('.$p.','.$p.','.$p.'\)/', '\1(\2,\5,\8)', $string);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 800 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

FIXME: ^^ not always, see start and value of list items

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1632 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

TODO: support SLASH syntax

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1719 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

:TODO: Is this htmlspecialchars() call really necessary?

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 2978 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

Assume that $this->keys is alphanumeric

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 3964 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

need to do PHP stuff. 99% of the time, this will be the case.

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 4215 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

unaffected by bugs, since UTF-8 support all characters

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 4236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

bugs.php.net/bug.php?id=48147 ' .

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 4284 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

You might be tempted to assume that the ASCII representation

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 4338 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

\* No bugs detected in iconv. \*/

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 4433 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

sequence? This assumes that there's no variable width

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 4470 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$this->table = unserialize(file\_get\_contents($file));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 5368 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$data = preg\_replace('#

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 5409 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

Fortunately, all we need to do is trigger an appropriate

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 5588 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

assume that if the user is calling this, the element

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 6657 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

:TODO:

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 7547 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

Hack:

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 7761 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

hack out something using XSLT, remove this stipulation

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7897 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace(

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7971 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$html = preg\_replace('#<\?.+?\?>#s', '', $html);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7978 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$html = preg\_replace('#<script[^>]\*>.\*?</script>#i', '', $html);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 8512 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

$fh = fopen($file, 'r');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 8512 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fh = fopen($file, 'r');

**STANDARD: Potentially Unsafe Code - fopen**

Line: 8532 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

$fh = fopen($file, 'r');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 8532 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fh = fopen($file, 'r');

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 9103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

defer to the schemes to do the right thing.

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 9506 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

kludge: browsers do funny things when the scheme but not the

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 9732 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

this will be useful when we need to do final rounding.

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 10333 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

escape sequences. So here is some dumb hack to

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 10528 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

we may want to do full case-insensitive libraries

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 11096 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

assumes URI doesn't have spaces in it

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 11953 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

assume that no font names contain commas in them

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 12076 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

str(c)spn assumes that the string was already well formed

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 12083 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

In the absence of innerHTML/cssText, these ugly

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 12179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

:TODO: optimization: test directly for !important and ! important

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 12317 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

assumes URI doesn't have spaces in it

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 12734 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

escaping because I don't know how to do that with regexps

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 13358 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

need to do checks on unusual encodings too

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 13411 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

since otherwise we have to assume browsers support

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 13644 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

this MUST be placed in post, as it assumes that any value in dir is valid

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 14340 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

the reasoning that it could only hack the SWF, not us.

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 14657 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$reg = preg\_replace("/$el/", '(,\\0)', $reg);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 14660 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$reg = preg\_replace("/([^,(|]\(+),/", '\\1', $reg);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 14663 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$reg = preg\_replace("/,\(/", '(', $reg);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 14804 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

ToDo: Make this more robust in the case of not ol/ul

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 14924 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

ToDo: Make configurable

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 14978 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

we assume that $children is not modified

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 15592 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

return unserialize(file\_get\_contents($file));

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 16669 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

so we're not going to do that subtlety. It might cause trouble

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 17152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

TODO: create custom child-definition for noscript that

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 17158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

TODO: convert this to new syntax, main problem is getting

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 18349 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

it was indeed needed. This prevents from needing to do a lookahead,

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 18655 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

HACK, see HTMLPurifier/Printer/ConfigForm.php

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 18849 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

if omitted, assume to be 'false'

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 18987 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$html = preg\_replace("/<($char)/i", '&lt;\\1', $html);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 20083 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

nodes. This enables error reporting to do its job

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 20129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

ToDo: I don't think it matters if it's def or

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 20306 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

assumed to be objects

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 20408 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

XXX fuckup

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 22417 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$uri->path = preg\_replace('/(?!^\+)[^\dx]/', '',

**STANDARD: Potentially Unsafe Code - eval**

Line: 22587 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$result = eval("\$var = $expr;");

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 22587 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\HTMLPurifier.standalone.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

$result = eval("\$var = $expr;");

**STANDARD: Potentially Unsafe Code - eval**

Line: 182 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\standalone\HTMLPurifier\ConfigSchema\InterchangeBuilder.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return eval('return array(' . $contents . ');');

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 182 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\standalone\HTMLPurifier\ConfigSchema\InterchangeBuilder.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

return eval('return array(' . $contents . ');');

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\standalone\HTMLPurifier\ConfigSchema\Builder\Xml.php

Kludge, although I suppose having a notion of a "root namespace"

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 327 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\standalone\HTMLPurifier\Filter\ExtractStyleBlocks.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$css = $this->\_tidy->print->plain();

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\standalone\HTMLPurifier\Filter\YouTube.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace($pre\_regex, $pre\_replace, $html);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 501 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\standalone\HTMLPurifier\Lexer\PH5P.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace('#^([' . $char\_class . ']+).\*#s', '\\1', substr($this->data, $start));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 4400 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\standalone\HTMLPurifier\Lexer\PH5P.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$token['name'] = preg\_replace('/[^a-z0-9-]/i', '', $token['name']);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 323 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\standalone\HTMLPurifier\Printer\ConfigForm.php

TODO does this need a break?

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 331 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\htmlpurifier\standalone\HTMLPurifier\Printer\ConfigForm.php

HACK

**MEDIUM: Potentially Unsafe Code - md5**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_find\_result.php

MD5 Hashing algorithm.

$md5\_ci = md5($ci . $ci);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_find\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $row["mb\_id"]; ?>">

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_request.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$userPhone = preg\_replace("/-/","" , $member['mb\_hp']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_request.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mid" value="<?php echo $mid ?>"> <!-- 필수 값 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_request.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="reqSvcCd" value="<?php echo $reqSvcCd ?>"> <!-- 필수 값 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_request.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mTxId" value="<?php echo $mTxId ?>"> <!-- 필수 값 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_request.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="authHash" value="<?php echo $authHash ?>"> <!-- 필수 값 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_request.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="flgFixedUser" value="<?php echo $flgFixedUser ?>"> <!-- 필수 값 Y/N 특정사용자 인증 요청 여부 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_request.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="userName" value="<?php echo $userName ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_request.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="userPhone" value="<?php echo $userPhone ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_request.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="userBirth" value="<?php echo $userBirth ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_request.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="userHash" value="<?php echo $userHash ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_request.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mbId" value="<?php echo $member['mb\_id'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_request.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="directAgency" value="<?php echo $\_GET['directAgency']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_request.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="successUrl" value="<?php echo $resultUrl; ?>"> <!-- 필수 값 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_request.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="failUrl" value="<?php echo $resultUrl; ?>"> <!-- 필수 값 -->

**MEDIUM: Potentially Unsafe Code - md5**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_result.php

MD5 Hashing algorithm.

$mb\_dupinfo = md5($ci . $ci);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_result.php

MD5 Hashing algorithm.

$md5\_cert\_no = md5($cert\_no);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_result.php

MD5 Hashing algorithm.

$hash\_data = md5($user\_name.$cert\_type.$birth\_day.$phone\_no.$md5\_cert\_no);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=cert\_type]").val("<?php echo $cert\_type; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=mb\_name]").val("<?php echo $user\_name; ?>").attr("readonly", true);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=mb\_hp]").val("<?php echo $phone\_no; ?>").attr("readonly", true);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\inicert\ini\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=cert\_no]").val("<?php echo $md5\_cert\_no; ?>");

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$font\_file=$fonts[mt\_rand(0, count($fonts)-1)];

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$odd=mt\_rand(0,1);

**STANDARD: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The code appears to use the mt\_rand function. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker, although this is partly mitigated by a seed that does not appear to be time-based.

$odd=mt\_rand(0,1);

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

+ mt\_rand(-round($fluctuation\_amplitude/3), round($fluctuation\_amplitude/3))

**STANDARD: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The code appears to use the mt\_rand function. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker, although this is partly mitigated by a seed that does not appear to be time-based.

+ mt\_rand(-round($fluctuation\_amplitude/3), round($fluctuation\_amplitude/3))

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$shift=mt\_rand(4,6);

**STANDARD: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The code appears to use the mt\_rand function. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker, although this is partly mitigated by a seed that does not appear to be time-based.

$shift=mt\_rand(4,6);

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

imagesetpixel($img, mt\_rand(0, $x-1), mt\_rand(10, $height-15), $white);

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

imagesetpixel($img, mt\_rand(0, $x-1), mt\_rand(10, $height-15), $black);

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$rand1=mt\_rand(750000,1200000)/10000000;

**STANDARD: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The code appears to use the mt\_rand function. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker, although this is partly mitigated by a seed that does not appear to be time-based.

$rand1=mt\_rand(750000,1200000)/10000000;

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$rand2=mt\_rand(750000,1200000)/10000000;

**STANDARD: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The code appears to use the mt\_rand function. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker, although this is partly mitigated by a seed that does not appear to be time-based.

$rand2=mt\_rand(750000,1200000)/10000000;

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$rand3=mt\_rand(750000,1200000)/10000000;

**STANDARD: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The code appears to use the mt\_rand function. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker, although this is partly mitigated by a seed that does not appear to be time-based.

$rand3=mt\_rand(750000,1200000)/10000000;

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$rand4=mt\_rand(750000,1200000)/10000000;

**STANDARD: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The code appears to use the mt\_rand function. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker, although this is partly mitigated by a seed that does not appear to be time-based.

$rand4=mt\_rand(750000,1200000)/10000000;

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$rand5=mt\_rand(0,31415926)/10000000;

**STANDARD: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The code appears to use the mt\_rand function. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker, although this is partly mitigated by a seed that does not appear to be time-based.

$rand5=mt\_rand(0,31415926)/10000000;

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$rand6=mt\_rand(0,31415926)/10000000;

**STANDARD: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The code appears to use the mt\_rand function. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker, although this is partly mitigated by a seed that does not appear to be time-based.

$rand6=mt\_rand(0,31415926)/10000000;

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$rand7=mt\_rand(0,31415926)/10000000;

**STANDARD: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The code appears to use the mt\_rand function. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker, although this is partly mitigated by a seed that does not appear to be time-based.

$rand7=mt\_rand(0,31415926)/10000000;

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$rand8=mt\_rand(0,31415926)/10000000;

**STANDARD: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The code appears to use the mt\_rand function. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker, although this is partly mitigated by a seed that does not appear to be time-based.

$rand8=mt\_rand(0,31415926)/10000000;

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$rand9=mt\_rand(330,420)/110;

**STANDARD: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The code appears to use the mt\_rand function. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker, although this is partly mitigated by a seed that does not appear to be time-based.

$rand9=mt\_rand(330,420)/110;

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$rand10=mt\_rand(330,450)/110;

**STANDARD: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha.lib.php

The code appears to use the mt\_rand function. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker, although this is partly mitigated by a seed that does not appear to be time-based.

$rand10=mt\_rand(330,450)/110;

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha\_mp3.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$contents .= file\_get\_contents($mp3);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo (get\_session("ss\_captcha\_key") === $captcha\_key) ? true : false;

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha\_session.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$keystring.=$allowed\_symbols[mt\_rand(0,strlen($allowed\_symbols)-1)];

**STANDARD: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcaptcha\kcaptcha\_session.php

The code appears to use the mt\_rand function. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker, although this is partly mitigated by a seed that does not appear to be time-based.

$keystring.=$allowed\_symbols[mt\_rand(0,strlen($allowed\_symbols)-1)];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\find\_kcpcert\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "dn\_hash 변조 위험있음 (".G5\_KCPCERT\_PATH.$bin\_exe." 파일에 실행권한이 있는지 확인하세요.)";

**MEDIUM: Potentially Unsafe Code - md5**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\find\_kcpcert\_result.php

MD5 Hashing algorithm.

$md5\_ci = md5($ci.$ci);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\find\_kcpcert\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'window.parent.$("#cert\_info").css("display", "");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\find\_kcpcert\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'window.parent.$("#kcp\_cert" ).css("display", "none");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\find\_kcpcert\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $row["mb\_id"]; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 189 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\find\_kcpcert\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $sbParam; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\kcpcert\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="form\_auth" method="post" action="<?php echo $cert\_url ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\kcpcert\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ordr\_idxx" value="<?php echo $ordr\_idxx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\kcpcert\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="site\_cd" value="<?php echo $site\_cd; ?>" />

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\kcpcert\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="Ret\_URL" value="<?php echo G5\_KCPCERT\_URL.$resultPage; ?>" />

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\kcpcert\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="up\_hash" value="<?php echo $up\_hash; ?>"/>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\kcpcert\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

frm.action=".<?php echo $resultPage; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\kcpcert\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

frm.action="<?php echo $cert\_url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\kcpcert\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "dn\_hash 변조 위험있음 (".G5\_KCPCERT\_PATH.$bin\_exe." 파일에 실행권한이 있는지 확인하세요.)";

**MEDIUM: Potentially Unsafe Code - md5**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\kcpcert\_result.php

MD5 Hashing algorithm.

$mb\_dupinfo = md5($ci.$ci);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\kcpcert\_result.php

MD5 Hashing algorithm.

$md5\_cert\_no = md5($cert\_no);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\kcpcert\_result.php

MD5 Hashing algorithm.

$hash\_data = md5($user\_name.$cert\_type.$birth\_day.$phone\_no.$md5\_cert\_no);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 194 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\kcpcert\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'window.parent.$("#cert\_info").css("display", "");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\kcpcert\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'window.parent.$("#kcp\_cert" ).css("display", "none");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 207 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\kcpcert\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $sbParam; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 228 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\kcpcert\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=cert\_type]").val("<?php echo $cert\_type; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 229 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\kcpcert\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=mb\_name]").val("<?php echo $user\_name; ?>").attr("readonly", true);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 230 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\kcpcert\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=mb\_hp]").val("<?php echo $phone\_no; ?>").attr("readonly", true);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 231 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\kcpcert\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=cert\_no]").val("<?php echo $md5\_cert\_no; ?>");

**STANDARD: Potentially Unsafe Code - exec**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\lib\ct\_cli\_lib.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$rt = exec( $exec\_cmd );

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\kcpcert\lib\ct\_cli\_lib.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

$rt = exec( $exec\_cmd );

**MEDIUM: Potentially Unsafe Code - md5**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyReq.php

MD5 Hashing algorithm.

$LGD\_HASHDATA = md5($LGD\_MID.$LGD\_BUYERSSN.$LGD\_TIMESTAMP.$LGD\_MERTKEY);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyReq.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<script language="javascript" src="<?php echo (isset($\_SERVER['HTTPS']) && $\_SERVER['HTTPS']=='on') ? 'https' : 'http'; ?>:

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyReq.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var LGD\_window\_type = "<?php echo $LGD\_WINDOW\_TYPE;?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyReq.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

lgdwin = open\_paymentwindow(document.getElementById(lgd\_form), '<?php echo $CST\_PLATFORM ?>', LGD\_window\_type);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyReq.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

lgdwin = openAuthonly( document.getElementById(lgd\_form), "<?php echo $CST\_PLATFORM; ?>", LGD\_window\_type, null );

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyReq.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.getElementById("LGD\_PAYINFO").action = "<?php echo $resultPage; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 175 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyReq.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form method="post" name ="LGD\_PAYINFO" id="LGD\_PAYINFO" action="<?php echo G5\_LGXPAY\_URL.$resultPage; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 181 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyReq.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<input type='hidden' name='$key' id='$key' value='$value'/>".PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - md5**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyRes.php

MD5 Hashing algorithm.

$mb\_dupinfo = md5($ci.$ci);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyRes.php

MD5 Hashing algorithm.

$md5\_cert\_no = md5($cert\_no);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyRes.php

MD5 Hashing algorithm.

$hash\_data = md5($user\_name.$cert\_type.$birth\_day.$phone\_no.$md5\_cert\_no);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyRes.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'window.parent.$("#cert\_info").css("display", "");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 169 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyRes.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'window.parent.$("#lgu\_cert" ).css("display", "none");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyRes.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'alert("인증요청이 취소 또는 실패하였습니다.\\n\\n코드 : '.$xpay->Response\_Code().' '.$xpay->Response\_Msg().'")';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 190 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyRes.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'window.parent.$("#cert\_info").css("display", "");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 191 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyRes.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'window.parent.$("#lgu\_cert" ).css("display", "none");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 192 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyRes.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'alert("인증요청이 실패하였습니다.\\n\\n코드 : '.$xpay->Response\_Code().' '.$xpay->Response\_Msg().'")';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 215 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyRes.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=cert\_type]").val("<?php echo $cert\_type; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 216 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyRes.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=mb\_name]").val("<?php echo $user\_name; ?>").attr("readonly", true);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 217 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyRes.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=mb\_hp]").val("<?php echo $phone\_no; ?>").attr("readonly", true);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 218 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\AuthOnlyRes.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=cert\_no]").val("<?php echo $md5\_cert\_no; ?>");

**MEDIUM: Potentially Unsafe Code - md5**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\find\_AuthOnlyRes.php

MD5 Hashing algorithm.

$md5\_ci = md5($ci.$ci);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\find\_AuthOnlyRes.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'window.parent.$("#cert\_info").css("display", "");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\find\_AuthOnlyRes.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'window.parent.$("#lgu\_cert" ).css("display", "none");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\find\_AuthOnlyRes.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'alert("인증요청이 취소 또는 실패하였습니다.\\n\\n코드 : '.$xpay->Response\_Code().' '.$xpay->Response\_Msg().'")';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 169 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\find\_AuthOnlyRes.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'window.parent.$("#cert\_info").css("display", "");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\find\_AuthOnlyRes.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'window.parent.$("#lgu\_cert" ).css("display", "none");'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\find\_AuthOnlyRes.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'alert("인증요청이 실패하였습니다.\\n\\n코드 : '.$xpay->Response\_Code().' '.$xpay->Response\_Msg().'")';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\find\_AuthOnlyRes.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $row["mb\_id"]; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\returnurl.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "LGD\_RESPCODE:" . $LGD\_RESPCODE . " ,LGD\_RESPMSG:" . $LGD\_RESPMSG;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\returnurl.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<input type='hidden' name='$key' id='$key' value='$value'>";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 455 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\JSON.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace(array(

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\patch.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "patch result = ".$xpay->Patch("lgdacom.conf");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "response code = " . $xpay->Response\_Code() . "<br>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "response msg = " . $xpay->Response\_Msg() . "<br>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "response count = " . $xpay->Response\_Count() . "<p>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "count = " . $i . "<br>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $name . " = " . $xpay->Response($name, $i) . "<br>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "response code = " . $xpay->Response\_Code() . "<br>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "response msg = " . $xpay->Response\_Msg() . "<p>";

**MEDIUM: Potentially Unsafe Code - md5**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

MD5 Hashing algorithm.

$this->log\_file = $this->config["log\_dir"] . "/log\_" . date("Ymd") . '\_' . substr(md5($random\_str), 0, 12) . ".log";

**MEDIUM: Potentially Unsafe Code - md5**

Line: 221 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

MD5 Hashing algorithm.

$charid = strtoupper(md5(uniqid(rand(), true)));

**STANDARD: Potentially Unsafe Code - fopen**

Line: 502 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

$fp = fopen($tmp\_file, "w");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 502 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fp = fopen($tmp\_file, "w");

**STANDARD: Potentially Unsafe Code - fopen**

Line: 525 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

$fp = fopen($tmp\_file, "r");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 525 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fp = fopen($tmp\_file, "r");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 627 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Binding to ip $ip\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 657 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error number: " .curl\_errno($this->ch) ."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 658 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error message: " .curl\_error($this->ch)."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 676 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Binding to ip $ip\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 687 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error number: " .curl\_errno($this->ch) ."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 688 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error message: " .curl\_error($this->ch)."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 706 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Binding to ip $ip\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 717 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error number: " .curl\_errno($this->ch) ."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 718 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error message: " .curl\_error($this->ch)."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 735 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Binding to ip $ip\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 755 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Url: $url\nPost String: $post\_string\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 769 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error number: " .curl\_errno($this->ch) ."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 770 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error message: " .curl\_error($this->ch)."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 787 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Binding to ip $ip\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 810 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Post String: $post\_string\n";

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 816 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

win hack

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 828 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error number: " .curl\_errno($this->ch) ."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 829 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error message: " .curl\_error($this->ch)."\n";

**MEDIUM: Potentially Unsafe Code - md5**

Line: 876 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

MD5 Hashing algorithm.

$LGD\_HASHDATA = md5($LGD\_MID.$LGD\_OID.$LGD\_AMOUNT.$LGD\_TIMESTAMP.$this->config[$LGD\_MID]);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 894 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

MD5 Hashing algorithm.

$LGD\_HASHDATA = md5($LGD\_MID.$LGD\_OID.$LGD\_AMOUNT.$LGD\_RESPCODE.$LGD\_TIMESTAMP.$this->config[$LGD\_MID]);

**MEDIUM: Potentially Unsafe Code - mcrypt\_ecb**

Line: 957 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

Deprecated function. Use mcrypt\_generic

$EncrytBuffer = mcrypt\_ecb(MCRYPT\_RIJNDAEL\_128,$key,$PlainBuffer,MCRYPT\_ENCRYPT);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 960 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "EncryptReturnValue = " . $EncryptReturnValue . "<BR>";

**MEDIUM: Potentially Unsafe Code - mcrypt\_ecb**

Line: 978 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

Deprecated function. Use mcrypt\_generic

$DecryptBuffer = mcrypt\_ecb(MCRYPT\_RIJNDAEL\_128,$key,$DecodeBuffer,MCRYPT\_DECRYPT);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 980 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "UnPaddString : ".$UnPaddString . "<BR>";

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$this->log\_file = $this->config["log\_dir"] . "/log\_" . date("Ymd") . '\_' . substr(md5(mt\_rand()), 0, 12) . ".log";

**MEDIUM: Potentially Unsafe Code - md5**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

MD5 Hashing algorithm.

$this->log\_file = $this->config["log\_dir"] . "/log\_" . date("Ymd") . '\_' . substr(md5(mt\_rand()), 0, 12) . ".log";

**STANDARD: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The code appears to use the mt\_rand function. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker, although this is partly mitigated by a seed that does not appear to be time-based.

$this->log\_file = $this->config["log\_dir"] . "/log\_" . date("Ymd") . '\_' . substr(md5(mt\_rand()), 0, 12) . ".log";

**STANDARD: Potentially Unsafe Code - fopen**

Line: 495 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

$fp = fopen($tmp\_file, "w");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 495 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fp = fopen($tmp\_file, "w");

**STANDARD: Potentially Unsafe Code - fopen**

Line: 516 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

$fp = fopen($tmp\_file, "r");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 516 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fp = fopen($tmp\_file, "r");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 694 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Binding to ip $ip\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 720 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Url: $url\nPost String: $post\_string\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 741 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error number: " .curl\_errno($this->ch) ."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 742 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error message: " .curl\_error($this->ch)."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 778 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Binding to ip $ip\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 794 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error number: " .curl\_errno($this->ch) ."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 795 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error message: " .curl\_error($this->ch)."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 832 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Binding to ip $ip\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 848 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error number: " .curl\_errno($this->ch) ."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 849 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error message: " .curl\_error($this->ch)."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 885 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Binding to ip $ip\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 911 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Url: $url\nPost String: $post\_string\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 931 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error number: " .curl\_errno($this->ch) ."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 932 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error message: " .curl\_error($this->ch)."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 970 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Binding to ip $ip\n";

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 982 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

hack to make it working

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1008 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Post String: $post\_string\n";

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1020 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

win hack

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1038 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error number: " .curl\_errno($this->ch) ."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1039 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\lgxpay\lgdacom\XPayClient4DB.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Error message: " .curl\_error($this->ch)."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\find\_hpcert2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if(preg\_match('~[^0-9a-zA-Z+/=]~', $encInfo, $match)) {echo "입력 값 확인이 필요합니다"; exit;}

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\find\_hpcert2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if(preg\_match('~[^0-9a-zA-Z+/=]~', $WEBPUBKEY, $match)) {echo "입력 값 확인이 필요합니다"; exit;}

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\find\_hpcert2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if(preg\_match('~[^0-9a-zA-Z+/=]~', $WEBSIGNATURE, $match)) {echo "입력 값 확인이 필요합니다"; exit;}

**STANDARD: Potentially Unsafe Code - exec**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\find\_hpcert2.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

exec($cmd, $out, $ret);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\find\_hpcert2.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

exec($cmd, $out, $ret);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\find\_hpcert2.php

MD5 Hashing algorithm.

$md5\_ci = md5($ci.$ci);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\find\_hpcert2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $row["mb\_id"]; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\find\_ipin2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if(preg\_match('~[^0-9a-zA-Z+/=]~', $encPsnlInfo, $match)) {echo "입력 값 확인이 필요합니다"; exit;}

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\find\_ipin2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if(preg\_match('~[^0-9a-zA-Z+/=]~', $WEBPUBKEY, $match)) {echo "입력 값 확인이 필요합니다"; exit;}

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\find\_ipin2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if(preg\_match('~[^0-9a-zA-Z+/=]~', $WEBSIGNATURE, $match)) {echo "입력 값 확인이 필요합니다"; exit;}

**STANDARD: Potentially Unsafe Code - exec**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\find\_ipin2.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

exec($cmd, $out, $ret);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\find\_ipin2.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

exec($cmd, $out, $ret);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\find\_ipin2.php

MD5 Hashing algorithm.

$md5\_ci = md5($ci.$ci);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\find\_ipin2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $row["mb\_id"]; ?>">

**STANDARD: Potentially Unsafe Code - exec**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\hpcert1.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

exec($cmd, $out, $ret);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\hpcert1.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

exec($cmd, $out, $ret);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\hpcert1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.form1.action = "<?php echo $commonSvlUrl; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\hpcert1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="rqst\_data" value="<?php echo $e\_rqstData; ?>"> <!-- 요청데이터 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\hpcert1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="target\_id" value="<?php echo $targetId; ?>"> <!-- 타겟ID -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\hpcert1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo ("<script>alert(\"$retcode\"); self.close();</script>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\hpcert2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if(preg\_match('~[^0-9a-zA-Z+/=]~', $encInfo, $match)) {echo "입력 값 확인이 필요합니다"; exit;}

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\hpcert2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if(preg\_match('~[^0-9a-zA-Z+/=]~', $WEBPUBKEY, $match)) {echo "입력 값 확인이 필요합니다"; exit;}

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\hpcert2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if(preg\_match('~[^0-9a-zA-Z+/=]~', $WEBSIGNATURE, $match)) {echo "입력 값 확인이 필요합니다"; exit;}

**STANDARD: Potentially Unsafe Code - exec**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\hpcert2.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

exec($cmd, $out, $ret);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\hpcert2.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

exec($cmd, $out, $ret);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\hpcert2.php

MD5 Hashing algorithm.

$mb\_dupinfo = md5($ci.$ci);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\hpcert2.php

MD5 Hashing algorithm.

$md5\_cert\_no = md5($req\_num);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\hpcert2.php

MD5 Hashing algorithm.

$hash\_data = md5($mb\_name.$cert\_type.$mb\_birth.$phone\_no.$md5\_cert\_no);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\hpcert2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=cert\_type]").val("<?php echo $cert\_type; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\hpcert2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=mb\_name]").val("<?php echo $mb\_name; ?>").attr("readonly", true);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\hpcert2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=mb\_hp]").val("<?php echo $phone\_no; ?>").attr("readonly", true);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\hpcert2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=cert\_no]").val("<?php echo $md5\_cert\_no; ?>");

**STANDARD: Potentially Unsafe Code - exec**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin1.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

exec($cmd, $out, $ret);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin1.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

exec($cmd, $out, $ret);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="kcbInForm" method="post" action="<?php echo $kcbForm\_action; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="IDPCODE" value="<?php echo $idpCode; ?>" />

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="IDPURL" value="<?php echo $idpUrl; ?>" />

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="CPCODE" value="<?php echo $cpCode; ?>" />

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="CPREQUESTNUM" value="<?php echo $curtime; ?>" />

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="RETURNURL" value="<?php echo $returnUrl; ?>" />

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="WEBPUBKEY" value="<?php echo $pubkey; ?>" />

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="WEBSIGNATURE" value="<?php echo $sig; ?>" />

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if(preg\_match('~[^0-9a-zA-Z+/=]~', $encPsnlInfo, $match)) {echo "입력 값 확인이 필요합니다"; exit;}

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if(preg\_match('~[^0-9a-zA-Z+/=]~', $WEBPUBKEY, $match)) {echo "입력 값 확인이 필요합니다"; exit;}

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if(preg\_match('~[^0-9a-zA-Z+/=]~', $WEBSIGNATURE, $match)) {echo "입력 값 확인이 필요합니다"; exit;}

**STANDARD: Potentially Unsafe Code - exec**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin2.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

exec($cmd, $out, $ret);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin2.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

exec($cmd, $out, $ret);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin2.php

MD5 Hashing algorithm.

$mb\_dupinfo = md5($ci.$ci);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin2.php

MD5 Hashing algorithm.

$md5\_cert\_no = md5($req\_num);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin2.php

MD5 Hashing algorithm.

$hash\_data = md5($mb\_name.$cert\_type.$mb\_birth.$md5\_cert\_no);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=cert\_type]").val("<?php echo $cert\_type; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=mb\_name]").val("<?php echo $mb\_name; ?>").attr("readonly", true);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\okname\ipin2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$opener.$("input[name=cert\_no]").val("<?php echo $md5\_cert\_no; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 345 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

public $Debugoutput = 'echo';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 663 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$this->Debugoutput = (strpos(PHP\_SAPI, 'cli') !== false ? 'echo' : 'html');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 719 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (!in\_array($this->Debugoutput, array('error\_log', 'html', 'echo')) and is\_callable($this->Debugoutput)) {

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 731 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

preg\_replace('/[\r\n]+/', '', $str),

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 740 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace('/\r\n?/ms', "\n", $str);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 874 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$name = trim(preg\_replace('/[\r\n]+/', '', $name));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 1016 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$name = trim(preg\_replace('/[\r\n]+/', '', $name));

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

@TODO: Write our own "idn\_to\_ascii" function for PHP <= 5.2.

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 1387 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

TODO: If possible, this should be changed to escapeshellarg. Needs thorough testing.

**STANDARD: Potentially Unsafe Code - popen**

Line: 1392 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

if (!@$mail = popen($sendmail, 'w')) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1392 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (!@$mail = popen($sendmail, 'w')) {

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 1392 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

if (!@$mail = popen($sendmail, 'w')) {

**STANDARD: Potentially Unsafe Code - popen**

Line: 1413 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

if (!@$mail = popen($sendmail, 'w')) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1413 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

if (!@$mail = popen($sendmail, 'w')) {

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 1413 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

if (!@$mail = popen($sendmail, 'w')) {

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 2168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

RFC1341 part 5 says 7bit is assumed if not specified

**MEDIUM: Potentially Unsafe Code - md5**

Line: 2206 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

MD5 Hashing algorithm.

return md5(uniqid(time()));

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 2372 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

@TODO would be nice to use php://temp streams here, but need to wrap for PHP < 5.1

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 2378 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

Workaround for PHP bug https://bugs.php.net/bug.php?id=69197

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2400 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$body = file\_get\_contents($signed);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 2445 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

RFC1341 part 5 says 7bit is assumed if not specified

**MEDIUM: Potentially Unsafe Code - md5**

Line: 2604 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

MD5 Hashing algorithm.

$inclhash = md5(serialize($attachment));

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 2635 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

RFC1341 part 5 says 7bit is assumed if not specified

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 2728 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$file\_buffer = file\_get\_contents($path);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2840 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$encoded = preg\_replace('/^(.\*)$/m', ' =?' . $this->CharSet . "?$encoding?\\1?=", $encoded);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 2856 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

Assume no multibytes (we can't handle without mbstring functions anyway)

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 2935 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace('/[^\r\n]{' . ($line\_max - 3) . '}[^=\r\n]{2}/', "$0=\r\n", $string);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 3439 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

MD5 Hashing algorithm.

$cid = md5($url) . '@phpmailer.0';

**MEDIUM: Potentially Unsafe Code - md5**

Line: 3464 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

MD5 Hashing algorithm.

$cid = md5($url) . '@phpmailer.0';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 3476 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$message = preg\_replace(

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 3522 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

trim(strip\_tags(preg\_replace('/<(head|title|style|script)[^>]\*>.\*?<\/\\1>/si', '', $html))),

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 3756 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace('/(\r\n|\r|\n)/ms', $breaktype, $text);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 3810 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$privKeyStr = !empty($this->DKIM\_private\_string) ? $this->DKIM\_private\_string : file\_get\_contents($this->DKIM\_private);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 3850 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$signHeader = preg\_replace('/\r\n\s+/', ' ', $signHeader);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 3855 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.phpmailer.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$value = preg\_replace('/\s{2,}/', ' ', $value);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 319 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.pop3.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Server -> Client: $response";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 334 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.pop3.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "Client -> Server: $string";

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 336 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.pop3.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

return fwrite($this->pop\_conn, $string, strlen($string));

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 374 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.pop3.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

print\_r($error);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.smtp.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

public $Debugoutput = 'echo';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 224 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.smtp.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (!in\_array($this->Debugoutput, array('error\_log', 'html', 'echo')) and is\_callable($this->Debugoutput)) {

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.smtp.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

preg\_replace('/[\r\n]+/', '', $str),

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 244 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.smtp.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace('/(\r\n|\r|\n)/ms', "\n", $str);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 564 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.smtp.php

MD5 Hashing algorithm.

return hash\_hmac('md5', $data, $key);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 577 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.smtp.php

MD5 Hashing algorithm.

$key = pack('H\*', md5($key));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 585 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.smtp.php

MD5 Hashing algorithm.

return md5($k\_opad . pack('H\*', md5($k\_ipad . $data)));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 900 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.smtp.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$detail = preg\_replace(

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 999 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.smtp.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$result = fwrite($this->smtp\_conn, $data);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\class.smtp.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

public function setDebugOutput($method = 'echo')

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\get\_oauth\_token.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'Refresh Token: ' . $token->getRefreshToken();

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\extras\EasyPeasyICS.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$uid = md5(uniqid(mt\_rand(), true)) . '@EasyPeasyICS';

**MEDIUM: Potentially Unsafe Code - md5**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\extras\EasyPeasyICS.php

MD5 Hashing algorithm.

$uid = md5(uniqid(mt\_rand(), true)) . '@EasyPeasyICS';

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\extras\EasyPeasyICS.php

hacksw/handcal//NONSGML v1.0//EN';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\extras\EasyPeasyICS.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $ics;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 406 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\extras\htmlfilter.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$attval = preg\_replace('/\"/s', '&quot;', $attval);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 564 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\extras\htmlfilter.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$newvalue = preg\_replace($valmatch, $valrepl, $attvalue);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 737 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\extras\htmlfilter.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$content = preg\_replace("|body(\s\*\{.\*?\})|si", ".bodyclass\\1", $content);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 752 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\extras\htmlfilter.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$content = preg\_replace("/^\s\*(@import.\*)$/mi","\n<!-- @import rules forbidden -->\n",$content);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 754 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\extras\htmlfilter.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$content = preg\_replace("/(\\\\)?u(\\\\)?r(\\\\)?l(\\\\)?/i", 'url', $content);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 784 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\extras\htmlfilter.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$contentNew = preg\_replace($match, $replace, $contentTemp);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 874 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\PHPMailer\extras\htmlfilter.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$body = preg\_replace('/&(\{.\*?\};)/si', '&amp;\\1', $body);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 553 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sms5\JSON.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace(array(

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sms5\sms5.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url = preg\_replace('#&amp;'.$starget.'=[0-9]\*#', '', $url) . '&amp;'.$starget.'=';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sms5\sms5.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$hp = preg\_replace("/^(01[016789])([0-9]{3,4})([0-9]{4})$/", $preg, $hp);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sms5\sms5.lib.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<script language='javascript'>alert('$msg');";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 216 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sms5\sms5.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$hp\_number = preg\_replace("/[^0-9]/","",$strDest[$i]['bk\_hp']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 243 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sms5\sms5.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$strDate=preg\_replace("/[^0-9]/","",$strDate);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 307 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sms5\sms5.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$msg = preg\_replace("/\r\n/", "\n", $msg);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 308 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sms5\sms5.lib.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$msg = preg\_replace("/\r/", "\n", $msg);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sns\view.sns.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

Kakao.init("<?php echo $config['cf\_kakao\_js\_apikey']; ?>");

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sns\view.sns.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

description: "<?php echo preg\_replace('/\r\n|\r|\n/','', strip\_tags(get\_text(cut\_str(strip\_tags($view['wr\_content']), 200), 1))); ?>",

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sns\view.sns.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<ul id="bo\_v\_sns" class="<?php echo $bo\_v\_sns\_class; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sns\view.sns.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $facebook\_url; ?>" target="\_blank" class="sns\_f"><img src="<?php echo G5\_SNS\_URL; ?>/icon/facebook.png" alt="페이스북으로 공유" width="20"><span>페이스북 공유</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sns\view.sns.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $twitter\_url; ?>" target="\_blank" class="sns\_t"><img src="<?php echo G5\_SNS\_URL; ?>/icon/twitter.png" alt="트위터로 공유" width="20"><span>트위터 공유</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sns\view.sns.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $gplus\_url; ?>" target="\_blank" class="sns\_g"><img src="<?php echo G5\_SNS\_URL; ?>/icon/gplus.png" alt="구글플러스로 공유" width="20"><span>구글+ 공유</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sns\view\_comment\_write.sns.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li class="sns\_li\_t '.($twitter\_user?'':'sns\_li\_off').'">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sns\view\_comment\_write.sns.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="'.$twitter\_url.'" id="twitter\_url" onclick="return false;" "><img src="'.G5\_SNS\_URL.'/icon/twitter.png" id="twitter\_icon" width="20"></a>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sns\view\_comment\_write.sns.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<script>$(function(){ $(document).on("click", "#twitter\_url", function(){ window.open(this.href, "twitter\_url", "width=600,height=250"); }); });</script>';

**HIGH: Potentially Unsafe Code - File Inclusion Vulnerability**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sns\twitter\connect.php

The code appears to use an unsafe file extension for an include statement which could allow an attacker to download it directly and read the uncompiled code.

include('html.inc');

**HIGH: Potentially Unsafe Code - File Inclusion Vulnerability**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sns\twitter\index.php

The code appears to use an unsafe file extension for an include statement which could allow an attacker to download it directly and read the uncompiled code.

include('html.inc');

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 475 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sns\twitter\twitteroauth\OAuth.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$rand = mt\_rand();

**MEDIUM: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 475 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sns\twitter\twitteroauth\OAuth.php

The code appears to use the mt\_rand and/or smt\_rand functions without a seed to generate pseudo-random values. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker.

$rand = mt\_rand();

**MEDIUM: Potentially Unsafe Code - md5**

Line: 477 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sns\twitter\twitteroauth\OAuth.php

MD5 Hashing algorithm.

return md5($mt . $rand);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 559 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sns\twitter\twitteroauth\OAuth.php

Service Providers MUST assume the protocol version to be 1.0 if this parameter is not present.

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 742 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\sns\twitter\twitteroauth\OAuth.php

parameters, has to do some unescaping

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\error.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<title>소셜 로그인 - <?php echo isset($provider) ? $provider : ''; ?></title>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\error.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h4>Error : <?php echo isset($code) ? $code : ''; ?></h4>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\error.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $get\_error; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\popup.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var login\_url = "<?php echo $get\_login\_url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\popup.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

window.opener.location.href = login\_url+"&provider=<?php echo $provider\_name; ?>";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\register\_member.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$user\_id = $user\_profile->sid ? preg\_replace("/[^0-9a-z\_]+/i", "", $user\_profile->sid) : get\_social\_convert\_id($user\_profile->identifier, $provider\_name);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\register\_member.php

MD5 Hashing algorithm.

$token = md5(uniqid(rand(), true));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\register\_member\_update.php

MD5 Hashing algorithm.

$mb\_password = md5(pack('V\*', rand(), rand(), rand(), rand()));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\register\_member\_update.php

MD5 Hashing algorithm.

if ($cert\_type == 'ipin' && get\_session('ss\_cert\_hash') == md5($mb\_name.$cert\_type.get\_session('ss\_cert\_birth').$md5\_cert\_no)) {

**MEDIUM: Potentially Unsafe Code - md5**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\register\_member\_update.php

MD5 Hashing algorithm.

} else if($cert\_type != 'ipin' && get\_session('ss\_cert\_hash') == md5($mb\_name.$cert\_type.get\_session('ss\_cert\_birth').$mb\_hp.$md5\_cert\_no)) {

**MEDIUM: Potentially Unsafe Code - md5**

Line: 175 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\register\_member\_update.php

MD5 Hashing algorithm.

if($cert\_type == 'ipin' && get\_session('ss\_cert\_hash') == md5($mb\_name.$cert\_type.get\_session('ss\_cert\_birth').$md5\_cert\_no)) {

**MEDIUM: Potentially Unsafe Code - md5**

Line: 177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\register\_member\_update.php

MD5 Hashing algorithm.

}else if($cert\_type != 'ipin' && get\_session('ss\_cert\_hash') == md5($mb\_name.$cert\_type.get\_session('ss\_cert\_birth').$mb\_hp.$md5\_cert\_no)) {

**MEDIUM: Potentially Unsafe Code - md5**

Line: 234 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\register\_member\_update.php

MD5 Hashing algorithm.

$mb\_md5 = md5(pack('V\*', rand(), rand(), rand(), rand()));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 293 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\register\_member\_update.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once ($member\_skin\_path.'/register\_form\_update.tail.skin.php');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 5 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\unlink.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$nonce = isset($\_POST['nonce']) ? preg\_replace('/[^\da-z]/i', '',$\_POST['nonce']) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 371 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\Auth.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo 'function redirect(){ window.top.location.href="' . $url . '"; }';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\Endpoint.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

print $output;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\Endpoint.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

print $output;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\Endpoint.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

print $output;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\Logger.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

print\_r($object, true) . PHP\_EOL,

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\Logger.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

print\_r($object, true) . PHP\_EOL

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\Providers\Facebook.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$token = md5(uniqid(mt\_rand(), true));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\Providers\Facebook.php

MD5 Hashing algorithm.

$token = md5(uniqid(mt\_rand(), true));

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\Providers\Facebook.php

if the provider identifier is not received, we assume the auth has failed

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\Providers\Facebook.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$coverOBJ = json\_decode(file\_get\_contents($coverInfoURL));

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 230 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\Providers\Naver.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$rand = mt\_rand();

**MEDIUM: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 230 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\Providers\Naver.php

The code appears to use the mt\_rand and/or smt\_rand functions without a seed to generate pseudo-random values. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker.

$rand = mt\_rand();

**MEDIUM: Potentially Unsafe Code - md5**

Line: 232 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\Providers\Naver.php

MD5 Hashing algorithm.

return md5($mt . $rand);

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\Providers\Payco.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$token = md5(uniqid(mt\_rand(), true));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\Providers\Payco.php

MD5 Hashing algorithm.

$token = md5(uniqid(mt\_rand(), true));

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 185 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\Providers\Payco.php

if the provider identifier is not received, we assume the auth has failed

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\Providers\Twitter.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $response;

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\Providers\Twitter.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$response = $this->api->post('statuses/update\_with\_media.json', array('status' => $status['message'], 'media[]' => file\_get\_contents($status['picture'])), null, null, true);

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 498 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\thirdparty\OAuth\OAuth.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$rand = mt\_rand();

**MEDIUM: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 498 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\thirdparty\OAuth\OAuth.php

The code appears to use the mt\_rand and/or smt\_rand functions without a seed to generate pseudo-random values. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker.

$rand = mt\_rand();

**MEDIUM: Potentially Unsafe Code - md5**

Line: 500 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\thirdparty\OAuth\OAuth.php

MD5 Hashing algorithm.

return md5($mt . $rand);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 582 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\thirdparty\OAuth\OAuth.php

Service Providers MUST assume the protocol version to be 1.0 if this parameter is not present.

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 776 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\thirdparty\OAuth\OAuth.php

parameters, has to do some unescaping

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\thirdparty\OpenID\LightOpenID.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$uri = rtrim(preg\_replace('#((?<=\?)|&)openid\.[^&]+#', '', $\_SERVER['REQUEST\_URI']), '?');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 560 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\Hybrid\thirdparty\OpenID\LightOpenID.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url = preg\_replace($this->xrds\_override\_pattern, $this->xrds\_override\_replacement, $url);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\functions.php

MD5 Hashing algorithm.

return strtolower($service).'\_'.hash('adler32', md5($identifier));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 286 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\functions.php

MD5 Hashing algorithm.

$setting['debug\_file'] = G5\_DATA\_PATH.'/tmp/social\_'.md5($\_SERVER['SERVER\_SOFTWARE'].$\_SERVER['SERVER\_ADDR']).'\_'.date('ymd').'.log';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 404 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\functions.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace("/[ #\&\+\-%@=\/\\\:;,\.'\"\^`~\\_|\!\?\\*$#<>()\[\]\{\}]/i", "", $nick);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 444 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\functions.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace('#\?.\*#', '?' . http\_build\_query($params), $url);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 540 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\functions.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo social\_return\_from\_provider\_page( $provider\_name, $login\_action\_url, $mb\_id, $mb\_password, $url, $use\_popup );

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 569 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\functions.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

window.opener.social\_link\_fn("<?php echo $provider\_name; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 620 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\functions.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

window.opener.social\_link\_fn("<?php echo $provider\_name; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 622 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\functions.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

window.opener.location.href = "<?php echo $register\_url; ?>";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 777 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\functions.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$host = preg\_replace('/:[0-9]+$/', '', $\_SERVER['HTTP\_HOST']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 897 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\functions.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $html;

**MEDIUM: Potentially Unsafe Code - md5**

Line: 1062 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\functions.php

MD5 Hashing algorithm.

return md5( $i . $action . $user . social\_get\_nonce($provider) );

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\g5\_endpoint.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$\_REQUEST['hauth\_start'] = preg\_replace('/[^a-zA-Z0-9\-\.\_]/i', '', $\_REQUEST[G5\_SOCIAL\_LOGIN\_START\_PARAM]);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\g5\_endpoint.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$\_REQUEST['hauth\_done'] = preg\_replace('/[^a-zA-Z0-9\-\.\_]/i', '', $\_REQUEST[G5\_SOCIAL\_LOGIN\_DONE\_PARAM]);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\loading.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<title>소셜 로그인 - <?php echo $provider; ?></title>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\loading.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td align="center" height="190px" valign="middle"><img src="<?php echo $img\_url;?>loading\_icon.gif" /></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\loading.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="loginform" method="post" action="<?php echo $login\_action\_url; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\loading.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="url" name="url" value="<?php echo $url ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\loading.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="provider" name="provider" value="<?php echo $provider ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\loading.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="mb\_id" name="mb\_id" value="<?php echo $mb\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\social\includes\loading.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="mb\_password" name="mb\_password" value="<?php echo $mb\_password ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\syndi\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<updated>{$feed\_updated}</updated>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\syndi\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<link rel=\"site\" href=\"" . G5\_URL . "\" title=\"{$cf\_title}\" />\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\syndi\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<id>{$id}</id>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\syndi\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<title><![CDATA[{$title}]]></title>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\syndi\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<name>{$author}</name>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\syndi\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<updated>{$updated}</updated>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\syndi\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<published>{$published}</published>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\syndi\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<link rel=\"via\" href=\"{$link\_href}\" title=\"{$link\_title}\" />\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\syndi\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<link rel=\"mobile\" href=\"{$id}\" />\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\syndi\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<content type=\"html\"><![CDATA[{$content}]]></content>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\syndi\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<summary type=\"text\"><![CDATA[{$summary}]]></summary>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\plugin\syndi\ping.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<category term=\"{$bo\_table}\" label=\"{$link\_title}\" />\n";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 4 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ajax.action.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$action = isset($\_REQUEST['action']) ? preg\_replace('/[^a-z0-9\_]/i', '', $\_REQUEST['action']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ajax.action.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$s\_cart\_id = preg\_replace('/[^a-z0-9\_\-]/i', '', get\_session('ss\_cart\_id'));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ajax.action.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$tmp\_cart\_id = preg\_replace('/[^a-z0-9\_\-]/i', '', $tmp\_cart\_id);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ajax.action.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$io\_id = isset($\_POST['io\_id'][$it\_id][$k]) ? preg\_replace(G5\_OPTION\_ID\_FILTER, '', $\_POST['io\_id'][$it\_id][$k]) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ajax.action.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$io\_type = isset($\_POST['io\_type'][$it\_id][$k]) ? preg\_replace('#[^01]#', '', $\_POST['io\_type'][$it\_id][$k]) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 278 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fcart" method="post" action="<?php echo $action\_url; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 280 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[]" value="<?php echo $it['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 281 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_name[]" value="<?php echo stripslashes($it['it\_name']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 282 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_price[]" value="<?php echo get\_price($it); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 283 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_stock[]" value="<?php echo get\_it\_stock\_qty($it['it\_id']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 284 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_type[<?php echo $it['it\_id']; ?>][]" value="0">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 285 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_id[<?php echo $it['it\_id']; ?>][]" value="">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 286 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_value[<?php echo $it['it\_id']; ?>][]" value="">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 287 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_price[<?php echo $it['it\_id']; ?>][]" value="">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 288 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ct\_qty[<?php echo $it['it\_id']; ?>][]" value="<?php echo $item\_ct\_qty; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 296 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_item;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ajax.coupondownload.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$cz\_id = isset($\_GET['cz\_id']) ? preg\_replace('#[^0-9]#', '', $\_GET['cz\_id']) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ajax.list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($theme\_cart\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="frmcartlist" id="sod\_bsk\_list" class="2017\_renewal\_itemform" method="post" action="<?php echo $cart\_action\_url; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="ct\_chk[<?php echo $i; ?>]" value="1" id="ct\_chk\_<?php echo $i; ?>" checked="checked" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ct\_chk\_<?php echo $i; ?>"><span></span><b class="sound\_only">상품</b></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sod\_img"><a href="<?php echo shop\_item\_url($row['it\_id']); ?>"><?php echo $image; ?></a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[<?php echo $i; ?>]" value="<?php echo $row['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_name[<?php echo $i; ?>]" value="<?php echo get\_text($row['it\_name']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $it\_name.$mod\_options; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 160 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($sum['qty']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig"><?php echo number\_format($row['ct\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig"><?php echo number\_format($point); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_dvr"><?php echo $ct\_send\_cost; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig text\_right"><span id="sell\_price\_<?php echo $i; ?>" class="total\_prc"><?php echo number\_format($sell\_price); ?></span></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($send\_cost); ?></strong> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 200 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($tot\_point); ?></strong> 점

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 205 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($tot\_price); ?></strong> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 216 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="records" value="<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 218 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo shop\_category\_url($continue\_ca\_id); ?>" class="btn01">쇼핑 계속하기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 222 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cart.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="cart-naverpay"><?php echo $naverpay\_request\_js.$naverpay\_button\_js; ?></div>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 5 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartoption.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$it\_id = isset($\_POST['it\_id']) ? preg\_replace($pattern, '', $\_POST['it\_id']) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[]" value="<?php echo $it['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="it\_price" value="<?php echo $row2['ct\_price']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ct\_send\_cost" value="<?php echo $row2['ct\_send\_cost']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_1;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_2;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="sit\_<?php echo $cls; ?>\_list">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_type[<?php echo $it['it\_id']; ?>][]" value="<?php echo $row['io\_type']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_id[<?php echo $it['it\_id']; ?>][]" value="<?php echo $row['io\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_value[<?php echo $it['it\_id']; ?>][]" value="<?php echo $row['ct\_option']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" class="io\_price" value="<?php echo $row['io\_price']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" class="io\_stock" value="<?php echo $it\_stock\_qty; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sit\_opt\_subj"><?php echo $row['ct\_option']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ct\_qty\_<?php echo $i; ?>" class="sound\_only">수량</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ct\_qty[<?php echo $it['it\_id']; ?>][]" value="<?php echo $row['ct\_qty']; ?>" id="ct\_qty\_<?php echo $i; ?>" class="num\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sit\_opt\_prc"><?php echo $io\_price; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var min\_qty = parseInt(<?php echo $it['it\_buy\_min\_qty']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var max\_qty = parseInt(<?php echo $it['it\_buy\_max\_qty']; ?>);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$tmp\_cart\_id = preg\_replace('/[^a-z0-9\_\-]/i', '', $tmp\_cart\_id);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 235 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$io\_id = isset($\_POST['io\_id'][$it\_id][$k]) ? preg\_replace(G5\_OPTION\_ID\_FILTER, '', $\_POST['io\_id'][$it\_id][$k]) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$io\_type = isset($\_POST['io\_type'][$it\_id][$k]) ? preg\_replace('#[^01]#', '', $\_POST['io\_type'][$it\_id][$k]) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 286 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$io\_id = isset($\_POST['io\_id'][$it\_id][$k]) ? preg\_replace(G5\_OPTION\_ID\_FILTER, '', $\_POST['io\_id'][$it\_id][$k]) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 287 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\cartupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$io\_type = isset($\_POST['io\_type'][$it\_id][$k]) ? preg\_replace('#[^01]#', '', $\_POST['io\_type'][$it\_id][$k]) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo shop\_category\_url($mshop\_ca\_row1['ca\_id']); ?>" class="cate\_li\_1\_a"><?php echo get\_text($mshop\_ca\_row1['ca\_name']); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo shop\_category\_url($mshop\_ca\_row2['ca\_id']); ?>"><?php echo get\_text($mshop\_ca\_row2['ca\_name']); ?></a>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\coupon.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($theme\_coupon\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\coupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\coupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="cou\_tit"><?php echo $row['cp\_subject']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\coupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="cou\_pri"><?php echo $cp\_price; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\coupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="cou\_target"><?php echo $cp\_target; ?> <i class="fa fa-angle-right" aria-hidden="true"></i></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\coupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="cou\_date"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo substr($row['cp\_start'], 2, 8); ?> ~ <?php echo substr($row['cp\_end'], 2, 8); ?></span>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\couponzone.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($skin\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\couponzone.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="sct\_nofile">'.str\_replace(G5\_PATH.'/', '', $skin\_file).' 파일을 찾을 수 없습니다.<br>관리자에게 알려주시면 감사하겠습니다.</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\event.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="sev\_admin"><a href="'.G5\_ADMIN\_URL.'/shop\_admin/itemeventform.php?w=u&amp;ev\_id='.$ev['ev\_id'].'" class="btn\_admin btn"><span class="sound\_only">이벤트 관리</span><i class="fa fa-cog fa-spin fa-fw"></i></a></div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\event.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var itemlist\_ca\_id = "<?php echo $ev\_id; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\event.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="sev\_himg" class="sev\_img"><img src="'.G5\_DATA\_URL.'/event/'.$ev\_id.'\_h" alt=""></div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\event.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="sev\_hhtml">'.conv\_content($ev['ev\_head\_html'], 1).'</div>';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\event.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$skin = preg\_replace('#\.+(\/|\\\)#', '', $skin);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\event.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\event.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div align="center">'.$ev['ev\_skin'].' 파일을 찾을 수 없습니다.<br>관리자에게 알려주시면 감사하겠습니다.</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\event.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_paging($config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page=");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\event.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="sev\_thtml">'.conv\_content($ev['ev\_tail\_html'], 1).'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\event.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="sev\_timg" class="sev\_img"><img src="'.G5\_DATA\_URL.'/event/'.$ev\_id.'\_t" alt=""></div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\item.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($ca['ca\_include\_head']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="sit\_admin"><a href="'.G5\_ADMIN\_URL.'/shop\_admin/itemform.php?w=u&amp;it\_id='.$it\_id.'" class="btn\_admin btn" title="상품 관리"><span class="sound\_only">상품 관리</span><i class="fa fa-cog fa-spin fa-fw"></i></a></div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="sit\_hhtml">'.conv\_content($it['it\_head\_html'], 1).'</div>';

**HIGH: Potentially Unsafe Code - User Controlled Variable Used on System Command Line**

Line: 176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\item.php

The application appears to allow the use of a user-controlled variable within backticks, allowing commandline execution.

$sql = " select count(\*) as cnt from `{$g5['g5\_shop\_item\_use\_table']}` where it\_id = '{$it\_id}' and is\_confirm = '1' ";

**HIGH: Potentially Unsafe Code - User Controlled Variable Used on System Command Line**

Line: 181 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\item.php

The application appears to allow the use of a user-controlled variable within backticks, allowing commandline execution.

$sql = " select count(\*) as cnt from `{$g5['g5\_shop\_item\_qa\_table']}` where it\_id = '{$it\_id}' ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 242 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="#sit\_inf" <?php if ($anc\_id == 'inf') echo 'class="sanchor\_on"'; ?>>상품정보</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 243 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="#sit\_use" <?php if ($anc\_id == 'use') echo 'class="sanchor\_on"'; ?>>사용후기 <span class="item\_use\_count"><?php echo $item\_use\_count; ?></span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 244 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="#sit\_qa" <?php if ($anc\_id == 'qa') echo 'class="sanchor\_on"'; ?>>상품문의 <span class="item\_qa\_count"><?php echo $item\_qa\_count; ?></span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 245 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($default['de\_baesong\_content']) { ?><li><a href="#sit\_dvr" <?php if ($anc\_id == 'dvr') echo 'class="sanchor\_on"'; ?>>배송정보</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 246 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($default['de\_change\_content']) { ?><li><a href="#sit\_ex" <?php if ($anc\_id == 'ex') echo 'class="sanchor\_on"'; ?>>교환정보</a></li><?php } ?>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 263 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\item.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($skin\_dir.'/item.form.skin.php');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 278 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo conv\_content($it['it\_tail\_html'], 1);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 283 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\item.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($ca['ca\_include\_tail']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemoption.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$it\_id = isset($\_POST['it\_id']) ? preg\_replace($pattern, '', $\_POST['it\_id']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemoption.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$opt\_id = isset($\_POST['opt\_id']) ? addslashes(sql\_real\_escape\_string(preg\_replace(G5\_OPTION\_ID\_FILTER, '', $\_POST['opt\_id']))) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemoption.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$idx = isset($\_POST['idx']) ? preg\_replace('#[^0-9]#', '', $\_POST['idx']) : 0;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemoption.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sel\_count = isset($\_POST['sel\_count']) ? preg\_replace('#[^0-9]#', '', $\_POST['sel\_count']) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemoption.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $str;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemqa.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url = preg\_replace('#&amp;page=[0-9]\*#', '', $url) . '&amp;page=';

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemqa.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql\_common = " from `{$g5['g5\_shop\_item\_qa\_table']}` where it\_id = '{$it\_id}' ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemqa.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo str\_replace(G5\_PATH.'/', '', $itemqa\_skin).' 스킨 파일이 존재하지 않습니다.';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemqa.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($itemqa\_skin);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 4 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemqaform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$w = isset($\_REQUEST['w']) ? preg\_replace('/[^0-9a-z]/i', '', trim($\_REQUEST['w'])) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemqaform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$iq\_id = isset($\_REQUEST['iq\_id']) ? preg\_replace('/[^0-9]/', '', trim($\_REQUEST['iq\_id'])) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemqaform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo str\_replace(G5\_PATH.'/', '', $itemqaform\_skin).' 스킨 파일이 존재하지 않습니다.';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemqaform.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($itemqaform\_skin);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemqaformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$iq\_question = preg\_replace('#<script(.\*?)>(.\*?)</script>#is', '', $iq\_question);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemqaformupdate.php

MD5 Hashing algorithm.

$sql = " select iq\_question, iq\_answer from {$g5['g5\_shop\_item\_qa\_table']} where iq\_id = '$iq\_id' and md5(concat(iq\_id,iq\_time,iq\_ip)) = '{$hash}' ";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemqaformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$data\_path = preg\_replace("/^\/.\*\/data/", "/data", $p['path']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemqaformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$data\_path = preg\_replace("/^\/.\*\/data/", "/data", $p['path']);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemqaformupdate.php

MD5 Hashing algorithm.

$sql = " delete from {$g5['g5\_shop\_item\_qa\_table']} where iq\_id = '$iq\_id' and md5(concat(iq\_id,iq\_time,iq\_ip)) = '{$hash}' ";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemqalist.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql\_common = " from `{$g5['g5\_shop\_item\_qa\_table']}` a join `{$g5['g5\_shop\_item\_table']}` b on (a.it\_id=b.it\_id) ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemqalist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo str\_replace(G5\_PATH.'/', '', $itemqalist\_skin).' 스킨 파일이 존재하지 않습니다.';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemqalist.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($itemqalist\_skin);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemrecommend.php

MD5 Hashing algorithm.

$token = md5(uniqid(rand(), true));

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemrecommend.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title']; ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemrecommend.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo $token; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemrecommend.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id" value="<?php echo $it\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title']; ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id" value="<?php echo $it\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $it['it\_name']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ss\_hp" value="<?php echo $member['mb\_hp']; ?>" id="ss\_hp" required class="required frm\_input full\_input" placeholder="휴대폰번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemstocksms.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea readonly><?php echo get\_text($config['cf\_privacy']) ?></textarea>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemuse.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$url = preg\_replace('#&amp;page=[0-9]\*#', '', $url) . '&amp;page=';

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemuse.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql\_common = " from `{$g5['g5\_shop\_item\_use\_table']}` where it\_id = '{$it\_id}' and is\_confirm = '1' ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemuse.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo str\_replace(G5\_PATH.'/', '', $itemuse\_skin).' 스킨 파일이 존재하지 않습니다.';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemuse.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($itemuse\_skin);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 4 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemuseform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$w = isset($\_REQUEST['w']) ? preg\_replace('/[^0-9a-z]/i', '', trim($\_REQUEST['w'])) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemuseform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$is\_id = isset($\_REQUEST['is\_id']) ? preg\_replace('/[^0-9]/', '', trim($\_REQUEST['is\_id'])) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemuseform.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo str\_replace(G5\_PATH.'/', '', $itemuseform\_skin).' 스킨 파일이 존재하지 않습니다.';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemuseform.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($itemuseform\_skin);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemuseformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$is\_content = preg\_replace('#<script(.\*?)>(.\*?)</script>#is', '', $is\_content);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemuseformupdate.php

MD5 Hashing algorithm.

$sql = " select is\_content from {$g5['g5\_shop\_item\_use\_table']} where is\_id = '$is\_id' and md5(concat(is\_id,is\_time,is\_ip)) = '{$hash}' ";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemuseformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$data\_path = preg\_replace("/^\/.\*\/data/", "/data", $p['path']);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemuseformupdate.php

MD5 Hashing algorithm.

$sql = " delete from {$g5['g5\_shop\_item\_use\_table']} where is\_id = '$is\_id' and md5(concat(is\_id,is\_time,is\_ip)) = '{$hash}' ";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemuselist.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql\_common = " from `{$g5['g5\_shop\_item\_use\_table']}` a join `{$g5['g5\_shop\_item\_table']}` b on (a.it\_id=b.it\_id) ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemuselist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo str\_replace(G5\_PATH.'/', '', $itemuselist\_skin).' 스킨 파일이 존재하지 않습니다.';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\itemuselist.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($itemuselist\_skin);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\largeimage.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($skin);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\largeimage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<p>'.str\_replace(G5\_PATH.'/', '', $skin).'파일이 존재하지 않습니다.</p>';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\list.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($ca['ca\_include\_head']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="sct\_admin"><a href="'.G5\_ADMIN\_URL.'/shop\_admin/categoryform.php?w=u&amp;ca\_id='.$ca\_id.'" class="btn\_admin btn"><span class="sound\_only">분류 관리</span><i class="fa fa-cog fa-spin fa-fw"></i></a></div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var itemlist\_ca\_id = "<?php echo $ca\_id; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="sct\_hhtml">'.conv\_content($ca['ca\_head\_html'], 1).'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="sct\_nofile">'.str\_replace(G5\_PATH.'/', '', $skin\_file).' 파일을 찾을 수 없습니다.<br>관리자에게 알려주시면 감사하겠습니다.</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_paging($config['cf\_write\_pages'], $page, $total\_page, $\_SERVER['SCRIPT\_NAME'].'?'.$qstr1.'&amp;page=');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="sct\_thtml">'.conv\_content($ca['ca\_tail\_html'], 1).'</div>';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\list.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

@include\_once($ca['ca\_include\_tail']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 169 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\list.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "\n<!-- {$ca['ca\_skin']} -->\n";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\listtype.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$type = isset($\_REQUEST['type']) ? preg\_replace("/[\<\>\'\"\\\'\\\"\%\=\(\)\s]/", "", $\_REQUEST['type']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\listtype.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$skin = preg\_replace('#\.+[\\\/]#', '', $skin);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\listtype.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\listtype.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div align="center">'.$skin.' 파일을 찾을 수 없습니다.<br>관리자에게 알려주시면 감사하겠습니다.</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\listtype.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_paging($config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page=");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mypage.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($theme\_mypage\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="my\_ov\_name"><?php echo get\_member\_profile\_img($member['mb\_id']); ?> <?php echo $member['mb\_name']; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><a href="<?php echo G5\_BBS\_URL; ?>/point.php" target="\_blank" class="win\_point"><?php echo number\_format($member['mb\_point']); ?></a> 점</dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><a href="<?php echo G5\_SHOP\_URL; ?>/coupon.php" target="\_blank" class="win\_coupon"><?php echo number\_format($cp\_count); ?></a></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == 'super') { ?><li><a href="<?php echo G5\_ADMIN\_URL; ?>/" class="btn\_admin">관리자</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo ($member['mb\_tel'] ? $member['mb\_tel'] : '미등록'); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo ($member['mb\_email'] ? $member['mb\_email'] : '미등록'); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo $member['mb\_today\_login']; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo $member['mb\_datetime']; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd id="smb\_my\_ovaddd"><?php echo sprintf("(%s%s)", $member['mb\_zip1'], $member['mb\_zip2']).' '.print\_address($member['mb\_addr1'], $member['mb\_addr2'], $member['mb\_addr3'], $member['mb\_addr\_jibeon']); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="smb\_my\_img"><?php echo $image; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="smb\_my\_tit"><a href="<?php echo shop\_item\_url($row['it\_id']); ?>"><?php echo stripslashes($row['it\_name']); ?></a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="smb\_my\_date"><?php echo $row['wi\_time']; ?></div>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderaddress.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($theme\_orderaddress\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="forderaddress" method="post" action="<?php echo $order\_action\_url; ?>" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ad\_id[<?php echo $i; ?>]" value="<?php echo $row['ad\_id'];?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk[]" value="<?php echo $i;?>" id="chk\_<?php echo $i;?>" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_<?php echo $i;?>"><span></span><b class="sound\_only">배송지선택</b></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ad\_subject<?php echo $i;?>" class="sound\_only">배송지명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ad\_subject[<?php echo $i; ?>]" id="ad\_subject<?php echo $i;?>" class="frm\_input" size="12" maxlength="20" value="<?php echo get\_text($row['ad\_subject']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_name"><?php echo get\_text($row['ad\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo print\_address($row['ad\_addr1'], $row['ad\_addr2'], $row['ad\_addr3'], $row['ad\_jibeon']); ?><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="ad\_tel"><?php echo $row['ad\_tel']; ?> / <?php echo $row['ad\_hp']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" value="<?php echo $addr; ?>" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>?w=d&amp;ad\_id=<?php echo $row['ad\_id']; ?>" class="del\_address mng\_btn">삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="ad\_default" value="<?php echo $row['ad\_id'];?>" id="ad\_default<?php echo $i;?>" <?php if($row['ad\_default']) echo 'checked="checked"';?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ad\_default<?php echo $i;?>" class="default\_lb mng\_btn">기본배송지</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderaddress.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ordercoupon.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$price = isset($\_POST['price']) ? preg\_replace('#[^0-9]#', '', $\_POST['price']) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ordercoupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="o\_cp\_id[]" value="<?php echo $row['cp\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ordercoupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="o\_cp\_prc[]" value="<?php echo $dc; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ordercoupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="o\_cp\_subj[]" value="<?php echo $row['cp\_subject']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ordercoupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_text($row['cp\_subject']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ordercoupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig"><?php echo number\_format($dc); ?></td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sw\_direct = isset($\_REQUEST['sw\_direct']) ? preg\_replace('/[^a-z0-9\_]/i', '', $\_REQUEST['sw\_direct']) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="forderform" id="forderform" method="post" action="<?php echo $order\_action\_url; ?>" autocomplete="off">

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$goods = preg\_replace("/\'|\"|\||\,|\&|\;/", "", $row['it\_name']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 192 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sod\_img"><?php echo $image; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 194 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[<?php echo $i; ?>]" value="<?php echo $row['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_name[<?php echo $i; ?>]" value="<?php echo get\_text($row['it\_name']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 196 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_price[<?php echo $i; ?>]" value="<?php echo $sell\_price; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 197 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cp\_id[<?php echo $i; ?>]" value="">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 198 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cp\_price[<?php echo $i; ?>]" value="0">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 200 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_notax[<?php echo $i; ?>]" value="<?php echo $row['it\_notax']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 202 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $it\_name; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 203 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $cp\_button; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 207 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo number\_format($sum['qty']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 208 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig text\_right"><?php echo number\_format($row['ct\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 209 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig text\_right"><span class="total\_price"><?php echo number\_format($sell\_price); ?></span></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 210 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig text\_right"><?php echo number\_format($point); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 211 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_dvr"><?php echo $ct\_send\_cost; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 241 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_price" value="<?php echo $tot\_sell\_price; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 242 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="org\_od\_price" value="<?php echo $tot\_sell\_price; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 243 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_send\_cost" value="<?php echo $send\_cost; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 248 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_goods\_name" value="<?php echo $goods; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 268 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="od\_name" value="<?php echo isset($member['mb\_name']) ? get\_text($member['mb\_name']) : ''; ?>" id="od\_name" required class="frm\_input required" maxlength="20"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 283 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="od\_tel" value="<?php echo get\_text($member['mb\_tel']); ?>" id="od\_tel" required class="frm\_input required" maxlength="20"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 287 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="od\_hp" value="<?php echo get\_text($member['mb\_hp']); ?>" id="od\_hp" class="frm\_input" maxlength="20"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 293 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_zip" value="<?php echo $member['mb\_zip1'].$member['mb\_zip2']; ?>" id="od\_zip" required class="frm\_input required" size="8" maxlength="6" placeholder="우편번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 295 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_addr1" value="<?php echo get\_text($member['mb\_addr1']) ?>" id="od\_addr1" required class="frm\_input frm\_address required" size="60" placeholder="기본주소">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 297 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_addr2" value="<?php echo get\_text($member['mb\_addr2']) ?>" id="od\_addr2" class="frm\_input frm\_address" size="60" placeholder="상세주소">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 300 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_addr3" value="<?php echo get\_text($member['mb\_addr3']) ?>" id="od\_addr3" class="frm\_input frm\_address" size="60" readonly="readonly" placeholder="참고항목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 302 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_addr\_jibeon" value="<?php echo get\_text($member['mb\_addr\_jibeon']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 307 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="od\_email" value="<?php echo $member['mb\_email']; ?>" id="od\_email" required class="frm\_input required" size="35" maxlength="100"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 319 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<option value="'.$sdate.'">'.$sdate.' ('.get\_yoil($sdate).')</option>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 390 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $addr\_list; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 449 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($tot\_sell\_price); ?></strong>원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 457 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($send\_cost); ?></strong>원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 461 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($tot\_point); ?></strong>점

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 466 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong id="ct\_tot\_price"><?php echo number\_format($tot\_price); ?></strong>원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 552 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="print\_price"><?php echo number\_format($tot\_price); ?></strong>원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 578 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="radio" id="od\_settle\_kakaopay" name="od\_settle\_case" value="KAKAOPAY" '.$checked.'> <label for="od\_settle\_kakaopay" class="kakaopay\_icon lb\_icon">KAKAOPAY</label>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 585 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="radio" id="od\_settle\_bank" name="od\_settle\_case" value="무통장" '.$checked.'> <label for="od\_settle\_bank" class="lb\_icon bank\_icon">무통장입금</label>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 592 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="radio" id="od\_settle\_vbank" name="od\_settle\_case" value="가상계좌" '.$checked.'> <label for="od\_settle\_vbank" class="lb\_icon vbank\_icon">'.$escrow\_title.'가상계좌</label>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 599 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="radio" id="od\_settle\_iche" name="od\_settle\_case" value="계좌이체" '.$checked.'> <label for="od\_settle\_iche" class="lb\_icon iche\_icon">'.$escrow\_title.'계좌이체</label>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 606 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="radio" id="od\_settle\_hp" name="od\_settle\_case" value="휴대폰" '.$checked.'> <label for="od\_settle\_hp" class="lb\_icon hp\_icon">휴대폰</label>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 613 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="radio" id="od\_settle\_card" name="od\_settle\_case" value="신용카드" '.$checked.'> <label for="od\_settle\_card" class="lb\_icon card\_icon">신용카드</label>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 658 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo run\_replace('shop\_orderform\_easypay\_buttons', implode(PHP\_EOL, $easypay\_prints), $easypay\_prints, $multi\_settle);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 663 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="radio" id="od\_settle\_inicislpay" data-case="lpay" name="od\_settle\_case" value="lpay" '.$checked.'> <label for="od\_settle\_inicislpay" class="inicis\_lpay lb\_icon">L.pay</label>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 669 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="radio" id="od\_settle\_inicis\_kakaopay" data-case="inicis\_kakaopay" name="od\_settle\_case" value="inicis\_kakaopay" '.$checked.' title="KG 이니시스 카카오페이"> <label for="od\_settle\_inicis\_kakaopay" class="inicis\_kakaopay lb\_icon">KG 이니시스 카카오페이<em></em></label>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 694 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="od\_temp\_point">사용 포인트(<?php echo $point\_unit; ?>점 단위)</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 695 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="max\_temp\_point" value="<?php echo $temp\_point; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 699 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><strong>보유포인트</strong><?php echo display\_point($member['mb\_point']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 700 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="max\_point\_box"><strong>최대 사용 가능 포인트</strong><em id="use\_max\_point"><?php echo display\_point($temp\_point); ?></em></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 729 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $bank\_account;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 776 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var form\_action\_url = "<?php echo $order\_action\_url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 790 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

{ it\_id: it\_id, sw\_direct: "<?php echo $sw\_direct; ?>" },

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var mb\_point = parseInt(<?php echo $member['mb\_point']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var max\_point = parseInt(<?php echo $default['de\_settle\_max\_point']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var point\_unit = parseInt(<?php echo $default['de\_settle\_point\_unit']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1317 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var point\_unit = parseInt(<?php echo $default['de\_settle\_point\_unit']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1328 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (temp\_point > <?php echo (int)$member['mb\_point']; ?>) {

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 1635 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$("#od\_hope\_date").datepicker({ changeMonth: true, changeYear: true, dateFormat: "yy-mm-dd", showButtonPanel: true, yearRange: "c-99:c+99", minDate: "+<?php echo (int)$default['de\_hope\_date\_after']; ?>d;", maxDate: "+<?php echo (int)$default['de\_hope\_date\_after'] + 6; ?>d;" });

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderformupdate.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql = "ALTER TABLE `{$g5['g5\_shop\_order\_table']}`

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 258 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_b\_zip = preg\_replace('/[^0-9]/', '', $od\_b\_zip);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 339 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 390 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 416 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 442 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 457 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time);

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 508 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderformupdate.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$od\_pwd = isset($\_POST['od\_pwd']) ? get\_encrypt\_string($\_POST['od\_pwd']) : get\_encrypt\_string(mt\_rand());

**STANDARD: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 508 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderformupdate.php

The code appears to use the mt\_rand function. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker, although this is partly mitigated by a seed that does not appear to be time-based.

$od\_pwd = isset($\_POST['od\_pwd']) ? get\_encrypt\_string($\_POST['od\_pwd']) : get\_encrypt\_string(mt\_rand());

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 531 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$od\_zip = preg\_replace('/[^0-9]/', '', $od\_zip);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 768 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$recv\_number = preg\_replace("/[^0-9]/", "", $recv\_numbers[$s]);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 769 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace("/[^0-9]/", "", $send\_numbers[$s]);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 791 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$recv\_number = preg\_replace("/[^0-9]/", "", $od\_hp);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 792 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace("/[^0-9]/", "", $default['de\_admin\_company\_tel']);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 851 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderformupdate.php

MD5 Hashing algorithm.

$uid = md5($od\_id.G5\_TIME\_YMDHIS.$REMOTE\_ADDR);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiry.php

MD5 Hashing algorithm.

$uid = md5($row['od\_id'].$row['od\_time'].$row['od\_ip']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiry.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiry.sub.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($theme\_inquiry\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiry.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (!$limit) { ?>총 <?php echo $cnt; ?> 건<?php } ?>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiry.sub.php

MD5 Hashing algorithm.

$uid = md5($row['od\_id'].$row['od\_time'].$row['od\_ip']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiry.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_SHOP\_URL; ?>/orderinquiryview.php?od\_id=<?php echo $row['od\_id']; ?>&amp;uid=<?php echo $uid; ?>"><?php echo $row['od\_id']; ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiry.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo substr($row['od\_time'],2,14); ?> (<?php echo get\_yoil($row['od\_time']); ?>)</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiry.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig"><?php echo $row['od\_cart\_count']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiry.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig text\_right"><?php echo display\_price($row['od\_cart\_price'] + $row['od\_send\_cost'] + $row['od\_send\_cost2']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiry.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig text\_right"><?php echo display\_price($row['od\_receipt\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiry.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig text\_right"><?php echo display\_price($row['od\_misu']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiry.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od\_status; ?></td>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquirycancel.php

MD5 Hashing algorithm.

$uid = md5($od['od\_id'].$od['od\_time'].$od['od\_ip']);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

MD5 Hashing algorithm.

$token = md5(uniqid(rand(), true));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

MD5 Hashing algorithm.

if (! (isset($od['od\_id']) && $od['od\_id']) || (!$is\_member && md5($od['od\_id'].$od['od\_time'].$od['od\_ip']) != get\_session('ss\_orderview\_uid'))) {

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($theme\_inquiryview\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sod\_fin\_no">주문번호 <strong><?php echo $od\_id; ?></strong></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td rowspan="<?php echo $rowspan; ?>" class="td\_imgsmall"><?php echo $image; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_itname" colspan="7" class="td\_bdno"><a href="<?php echo shop\_item\_url($row['it\_id']); ?>"><?php echo $row['it\_name']; ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_itopt" class="td\_bdno"><?php echo get\_text($opt['ct\_option']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_itqty" class="td\_mngsmall"><?php echo number\_format($opt['ct\_qty']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_itprice" class="td\_numbig text\_right"><?php echo number\_format($opt\_price); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_itsum" class="td\_numbig text\_right"><?php echo number\_format($sell\_price); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_itpt" class="td\_numbig text\_right"><?php echo number\_format($point); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 160 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_itsd" class="td\_dvr"><?php echo $ct\_send\_cost; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_itst" class="td\_mngsmall"><?php echo $opt['ct\_status']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 266 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od\_id; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 270 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od['od\_time']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 274 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo check\_pay\_name\_replace($od['od\_settle\_case'], $od, 1); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 278 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od\_receipt\_price; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 286 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od['od\_receipt\_time']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 296 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><?php echo $app\_no\_subj; ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 297 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $app\_no; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 308 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_deposit\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 312 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_bank\_account']); ?></td>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 329 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

MD5 Hashing algorithm.

$LGD\_HASHDATA = md5($LGD\_MID.$LGD\_TID.$LGD\_MERTKEY);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 338 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $hp\_receipt\_script; ?>">영수증 출력</a>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 348 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

MD5 Hashing algorithm.

$LGD\_HASHDATA = md5($LGD\_MID.$LGD\_TID.$LGD\_MERTKEY);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 357 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $card\_receipt\_script; ?>">영수증 출력</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 367 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $card\_receipt\_script; ?>">영수증 출력</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 381 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_point($od['od\_receipt\_point']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 392 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_price($od['od\_refund\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 433 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $cash\_receipt\_script; ?>" class="btn\_frmline">현금영수증 확인하기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 439 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="window.open('<?php echo G5\_SHOP\_URL; ?>/taxsave.php?od\_id=<?php echo $od\_id; ?>', 'taxsave', 'width=550,height=400,scrollbars=1,menus=0');" class="btn\_frmline">현금영수증을 발급하시려면 클릭하십시오.</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 460 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 464 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_tel']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 468 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_hp']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 472 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text(sprintf("(%s%s)", $od['od\_zip1'], $od['od\_zip2']).' '.print\_address($od['od\_addr1'], $od['od\_addr2'], $od['od\_addr3'], $od['od\_addr\_jibeon'])); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 476 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_email']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 492 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_b\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 496 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_b\_tel']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 500 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_b\_hp']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 504 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text(sprintf("(%s%s)", $od['od\_b\_zip1'], $od['od\_b\_zip2']).' '.print\_address($od['od\_b\_addr1'], $od['od\_b\_addr2'], $od['od\_b\_addr3'], $od['od\_b\_addr\_jibeon'])); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 513 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo substr($od['od\_hope\_date'],0,10).' ('.get\_yoil($od['od\_hope\_date']).')' ;?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 521 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo conv\_content($od['od\_memo'], 0); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 542 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od['od\_delivery\_company']; ?> <?php echo get\_delivery\_inquiry($od['od\_delivery\_company'], $od['od\_invoice'], 'dvr\_link'); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 546 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od['od\_invoice']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 550 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od['od\_invoice\_time']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 573 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($od['od\_cart\_price']); ?> 원</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 578 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($od['od\_cart\_coupon']); ?> 원</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 585 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($od['od\_coupon']); ?> 원</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 592 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($od['od\_send\_cost']); ?> 원</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 599 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($od['od\_send\_coupon']); ?> 원</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 606 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($od['od\_send\_cost2']); ?> 원</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 612 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($od['od\_cancel\_price']); ?> 원</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 618 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($tot\_price); ?> 원</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 622 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($tot\_point); ?> 점</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 632 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo display\_price($tot\_price); ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 638 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<strong>'.display\_price($misu\_price).'</strong>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 644 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $wanbul; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 647 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><span class="title"><i class="fa fa-angle-right" aria-hidden="true"></i> 포인트 결제</span><?php echo number\_format($od['od\_receipt\_point']); ?> 점</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 648 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><span class="title"><i class="fa fa-angle-right" aria-hidden="true"></i> 실결제</span><?php echo number\_format($od['od\_receipt\_price']); ?> 원</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 666 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_id" value="<?php echo $od['od\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 667 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo $token; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 703 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="e\_trade\_no" value="<?php echo $od['od\_tno']; ?>"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 707 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="deposit\_no" value="<?php echo $deposit\_no; ?>"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 711 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="req\_name" value="<?php echo $od['od\_deposit\_name']; ?>"></td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderitemcoupon.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$it\_id = isset($\_POST['it\_id']) ? preg\_replace($pattern, '', $\_POST['it\_id']) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderitemcoupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="f\_cp\_id[]" value="<?php echo $row['cp\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderitemcoupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="f\_cp\_prc[]" value="<?php echo $dc; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderitemcoupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="f\_cp\_subj[]" value="<?php echo $row['cp\_subject']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderitemcoupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_text($row['cp\_subject']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\orderitemcoupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig"><?php echo number\_format($dc); ?></td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 4 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ordersendcost.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$code = isset($\_POST['zipcode']) ? preg\_replace('#[^0-9]#', '', $\_POST['zipcode']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ordersendcostcoupon.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$price = isset($\_POST['price']) ? preg\_replace('#[^0-9]#', '', $\_POST['price']) : 0;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ordersendcostcoupon.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_cost = isset($\_POST['send\_cost']) ? preg\_replace('#[^0-9]#', '', $\_POST['send\_cost']) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ordersendcostcoupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="s\_cp\_id[]" value="<?php echo $row['cp\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ordersendcostcoupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="s\_cp\_prc[]" value="<?php echo $dc; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ordersendcostcoupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="s\_cp\_subj[]" value="<?php echo $row['cp\_subject']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ordersendcostcoupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_text($row['cp\_subject']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\ordersendcostcoupon.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_numbig"><?php echo number\_format($dc); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpay.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_paging($config['cf\_write\_pages'], $page, $total\_page, $\_SERVER['SCRIPT\_NAME'].'?'.$qstr.'&amp;page=');

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 4 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayform.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$pp\_id = isset($\_REQUEST['pp\_id']) ? preg\_replace('/[^0-9]/', '', $\_REQUEST['pp\_id']) : 0;

**MEDIUM: Potentially Unsafe Code - md5**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayform.php

MD5 Hashing algorithm.

$hash\_data = md5($pp['pp\_id'].$pp['pp\_price'].$pp['pp\_time']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="forderform" id="forderform" method="post" action="<?php echo $order\_action\_url; ?>" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="pp\_id" value="<?php echo $pp['pp\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="2"><?php echo conv\_content($pp['pp\_content'], 0); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="2"><?php echo display\_price($pp['pp\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="pp\_name" value="<?php echo get\_text($pp['pp\_name']); ?>" id="pp\_name" required class="required frm\_input"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="pp\_hp" value="<?php echo get\_text($member['mb\_hp']); ?>" id="pp\_hp" required class="required frm\_input"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="2"><input type="text" name="pp\_email" value="<?php echo $member['mb\_email']; ?>" id="pp\_email" required class="required frm\_input" size="30"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="radio" id="pp\_settle\_vbank" name="pp\_settle\_case" value="가상계좌" '.$checked.'> <label for="pp\_settle\_vbank" class="lb\_icon"><span></span>'.$escrow\_title.'가상계좌</label>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="radio" id="pp\_settle\_iche" name="pp\_settle\_case" value="계좌이체" '.$checked.'> <label for="pp\_settle\_iche" class="lb\_icon"><span></span>'.$escrow\_title.'계좌이체</label>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="radio" id="pp\_settle\_hp" name="pp\_settle\_case" value="휴대폰" '.$checked.'> <label for="pp\_settle\_hp" class="lb\_icon"><span></span>휴대폰</label>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="radio" id="pp\_settle\_card" name="pp\_settle\_case" value="신용카드" '.$checked.'> <label for="pp\_settle\_card" class="lb\_icon"><span></span>신용카드</label>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayform.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var tot\_price = <?php echo (int)$pp['pp\_price']; ?>;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 5 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$pp\_id = $\_POST['pp\_id'] = isset($\_POST['pp\_id']) ? preg\_replace('/[^0-9]/', '', $\_POST['pp\_id']) : 0;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$good\_mny = $\_POST['good\_mny'] = isset($\_POST['good\_mny']) ? preg\_replace('/[^0-9]/', '', $\_POST['good\_mny']) : 0;

**MEDIUM: Potentially Unsafe Code - md5**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayformupdate.php

MD5 Hashing algorithm.

$hash\_data = md5($pp\_id.$good\_mny.$pp['pp\_time']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$pp\_receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$pp\_receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayformupdate.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$pp\_receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 234 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayformupdate.php

MD5 Hashing algorithm.

$uid = md5($pp['pp\_id'].$pp['pp\_time'].$\_SERVER['REMOTE\_ADDR']);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 4 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$pp\_id = isset($\_REQUEST['pp\_id']) ? preg\_replace('/[^0-9]/', '', $\_REQUEST['pp\_id']) : 0;

**MEDIUM: Potentially Unsafe Code - md5**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

MD5 Hashing algorithm.

if (! (isset($pp['pp\_id']) && $pp['pp\_id']) || (md5($pp['pp\_id'].$pp['pp\_time'].$\_SERVER['REMOTE\_ADDR']) != get\_session('ss\_personalpay\_uid'))) {

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p id="sod\_fin\_no">개인결제번호 <strong><?php echo $pp\_id; ?></strong></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $pp['od\_id']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $pp['pp\_settle\_case']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $pp\_receipt\_price; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo is\_null\_time($pp['pp\_receipt\_time']) ? '' : $pp['pp\_receipt\_time']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><?php echo $app\_no\_subj; ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $app\_no; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($pp['pp\_deposit\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($pp['pp\_bank\_account']); ?></td>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

MD5 Hashing algorithm.

$LGD\_HASHDATA = md5($LGD\_MID.$LGD\_TID.$LGD\_MERTKEY);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $hp\_receipt\_script; ?>">영수증 출력</a>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

MD5 Hashing algorithm.

$LGD\_HASHDATA = md5($LGD\_MID.$LGD\_TID.$LGD\_MERTKEY);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $card\_receipt\_script; ?>">영수증 출력</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 234 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $cash\_receipt\_script; ?>" class="btn\_frmline">현금영수증 확인하기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 240 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="window.open('<?php echo G5\_SHOP\_URL; ?>/taxsave.php?tx=personalpay&od\_id=<?php echo $pp\_id; ?>', 'taxsave', 'width=550,height=400,scrollbars=1,menus=0');" class="btn\_frmline">현금영수증을 발급하시려면 클릭하십시오.</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 260 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo display\_price($pp['pp\_price']); ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 266 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<strong>'.display\_price($misu\_price).'</strong>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 272 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $wanbul; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 293 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="e\_trade\_no" value="<?php echo $pp['pp\_tno']; ?>" size="80"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 297 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="deposit\_no" value="<?php echo $deposit\_no; ?>" size="80"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 301 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\personalpayresult.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="req\_name" value="<?php echo $pp['pp\_deposit\_name']; ?>" size="80"></td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\search.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$qcaid = isset($\_GET['qcaid']) ? preg\_replace('#[^a-z0-9]#i', '', trim($\_GET['qcaid'])) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\search.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$qfrom = isset($\_GET['qfrom']) ? preg\_replace('/[^0-9]/', '', trim($\_GET['qfrom'])) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\search.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$qto = isset($\_GET['qto']) ? preg\_replace('/[^0-9]/', '', trim($\_GET['qto'])) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\search.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$qsort = preg\_replace("/[\<\>\'\"\\\'\\\"\%\=\(\)\s]/", "", $qsort);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\search.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo str\_replace(G5\_PATH.'/', '', $search\_skin).' 스킨 파일이 존재하지 않습니다.';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\search.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($search\_skin);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $receipt\_time);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

$logfile = fopen( $INIpayHome . "/log/result.log", "a+" );

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$logfile = fopen( $INIpayHome . "/log/result.log", "a+" );

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile,"\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile,"ID\_MERCHANT : ".$id\_merchant."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile,"NO\_TID : ".$no\_tid."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile,"NO\_OID : ".$no\_oid."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile,"NO\_VACCT : ".$no\_vacct."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile,"AMT\_INPUT : ".$amt\_input."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile,"NM\_INPUTBANK : ".$nm\_inputbank."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile,"NM\_INPUT : ".$nm\_input."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile,"\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile,"전체 결과값"."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $msg\_id."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $no\_tid."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $no\_oid."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $id\_merchant."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $cd\_bank."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $dt\_trans."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $tm\_trans."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $no\_msgseq."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $type\_msg."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $cl\_close."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $cl\_kor."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $no\_msgmanage."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $no\_vacct."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $amt\_input."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $amt\_check."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $nm\_inputbank."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $nm\_input."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $dt\_inputstd."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $dt\_calculstd."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, $flg\_close."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_inicis\_common.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite( $logfile, "\r\n");

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_kcp\_common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $tx\_tm);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_lg\_common.php

MD5 Hashing algorithm.

$LGD\_HASHDATA2 = md5($LGD\_MID.$LGD\_OID.$LGD\_AMOUNT.$LGD\_RESPCODE.$LGD\_TIMESTAMP.$LGD\_MERTKEY);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_lg\_common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$receipt\_time = preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $LGD\_PAYDATE);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\settle\_lg\_common.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $resultMSG;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="hd\_h1"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_SHOP\_URL; ?>/"><img src="<?php echo G5\_DATA\_URL; ?>/common/logo\_img" alt="<?php echo $config['cf\_title']; ?>"></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="q" value="<?php echo stripslashes(get\_text(get\_search\_string($q))); ?>" id="sch\_str" required placeholder="검색어를 입력해주세요">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 214 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="wrapper" class="<?php echo implode(' ', $wrapper\_class); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 259 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="<?php echo implode(' ', $content\_class); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 260 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ((!$bo\_table || $w == 's' ) && !defined('\_INDEX\_')) { ?><div id="wrapper\_title"><?php echo $g5['title'] ?></div><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>회사명</b> <?php echo $default['de\_admin\_company\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>주소</b> <?php echo $default['de\_admin\_company\_addr']; ?></span><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>사업자 등록번호</b> <?php echo $default['de\_admin\_company\_saupja\_no']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>대표</b> <?php echo $default['de\_admin\_company\_owner']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>전화</b> <?php echo $default['de\_admin\_company\_tel']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>팩스</b> <?php echo $default['de\_admin\_company\_fax']; ?></span><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <span><b>운영자</b> <?php echo $admin['mb\_name']; ?></span><br> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>통신판매업신고번호</b> <?php echo $default['de\_admin\_tongsin\_no']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>개인정보 보호책임자</b> <?php echo $default['de\_admin\_info\_name']; ?></span><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($default['de\_admin\_buga\_no']) echo '<span><b>부가통신사업신고번호</b> '.$default['de\_admin\_buga\_no'].'</span>'; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="ft\_copy">Copyright &copy; 2001-2013 <?php echo $default['de\_admin\_company\_name']; ?>. All Rights Reserved.</div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $config['cf\_analytics'];

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\wishlist.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($theme\_wishlist\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sod\_ws\_img"><a href="<?php echo shop\_item\_url($row['it\_id']); ?>"><?php echo $image; ?></a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_it\_id[<?php echo $i; ?>]" value="1" id="chk\_it\_id\_<?php echo $i; ?>" onclick="out\_cd\_check(this, '<?php echo $out\_cd; ?>');" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_it\_id\_<?php echo $i; ?>"><span></span><b class="sound\_only"><?php echo $row['it\_name']; ?></b></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[<?php echo $i; ?>]" value="<?php echo $row['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_type[<?php echo $row['it\_id']; ?>][0]" value="0">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_id[<?php echo $row['it\_id']; ?>][0]" value="">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_value[<?php echo $row['it\_id']; ?>][0]" value="<?php echo $row['it\_name']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ct\_qty[<?php echo $row['it\_id']; ?>][0]" value="1">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo shop\_item\_url($row['it\_id']); ?>" class="info\_link"><?php echo stripslashes($row['it\_name']); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="info\_date"><?php echo $row['wi\_time']; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\wishlist.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./wishupdate.php?w=d&amp;wi\_id=<?php echo $row['wi\_id']; ?>" class="wish\_del"><i class="fa fa-trash" aria-hidden="true"></i><span class="sound\_only">삭제</span></a>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\\_common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sort = preg\_replace("/[\<\>\'\"\\\'\\\"\%\=\(\)\s]/", "", $sort);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\inipay\_cancel.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ini\_oid = preg\_replace('/[^a-z0-9\_\-]/i', '', get\_session('ss\_order\_id'));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\inipay\_cancel.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$tno = preg\_replace('/[^a-z0-9\_\-]/i', '', $tno);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\inipay\_cancel.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

P\_AUTH\_DT = '".preg\_replace('/[^0-9]/', '', G5\_TIME\_YMDHIS)."' where oid = '$ini\_oid' and P\_TID = '$tno' ";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\inipay\_cancel.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

P\_AUTH\_DT = '".preg\_replace('/[^0-9]/', '', G5\_TIME\_YMDHIS)."' ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\inistdpay\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $httpUtil->errormsg;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\inistdpay\_result.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$oid = preg\_replace('/[^A-Za-z0-9\-\_]/', '', $resultMap['MOID']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\inistdpay\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $s;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\inistdpay\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $httpUtil->errormsg;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 189 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\inistdpay\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<pre>", $netcancelResultString . "</pre>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 209 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\inistdpay\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $s;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\inistdpay\_return.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$orderNumber = isset($\_POST['orderNumber']) ? preg\_replace("/[ #\&\+%@=\/\\\:;,\.'\"\^`~|\!\?\\*$#<>()\[\]\{\}]/i", "", strip\_tags($\_POST['orderNumber'])) : 0;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\lpay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mid" value="<?php echo $mid; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\lpay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="oid" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\lpay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="acceptmethod" value="<?php echo $acceptmethod; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\lpay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="returnUrl" value="<?php echo $returnUrl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\lpay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="closeUrl" value="<?php echo $closeUrl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\lpay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="popupUrl" value="<?php echo $popupUrl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\lpay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="nointerest" value="<?php echo $cardNoInterestQuota; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\lpay\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="quotabase" value="<?php echo $cardQuotaBase; ?>">

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\makesignature.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$price = preg\_replace('#[^0-9]#', '', $\_POST['price']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_mny" value="<?php echo $tot\_price; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_tax\_mny" value="<?php echo $comm\_tax\_mny; ?>"> <!-- 과세금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_vat\_mny" value="<?php echo $comm\_vat\_mny; ?>"> <!-- 부가세 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_free\_mny" value="<?php echo $comm\_free\_mny; ?>"> <!-- 비과세 금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mid" value="<?php echo $mid; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="oid" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="goodname" value="<?php echo $goods; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="price" value="<?php echo $tot\_price; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="acceptmethod" value="<?php echo $acceptmethod; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="returnUrl" value="<?php echo $returnUrl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="closeUrl" value="<?php echo $closeUrl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="popupUrl" value="<?php echo $popupUrl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="nointerest" value="<?php echo $cardNoInterestQuota; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="quotabase" value="<?php echo $cardQuotaBase; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="tax" value="<?php echo $comm\_vat\_mny; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="taxfree" value="<?php echo $comm\_free\_mny; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title']; ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od\_id; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $goods\_name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od\_name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od\_email; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od\_tel; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="tx" value="<?php echo $tx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_id" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $trad\_time; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="buyeremail" id="buyeremail" value="<?php echo $od\_email; ?>" required class="required frm\_input" size="30"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($amt\_tot); ?>원</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($amt\_sup); ?>원<!-- ((거래금액 총합 \* 10) / 11) --></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 175 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($amt\_svc); ?>원</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($amt\_tax); ?>원<!-- 거래금액 총합 - 공급가액 - 봉사료 --></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $inipay->GetResult('ResultCode'); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo iconv\_utf8($inipay->GetResult('ResultMsg')); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $inipay->GetResult('TID'); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $inipay->GetResult('ApplNum'); ?></td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 175 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_result.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

<td><?php echo preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6",$inipay->GetResult('ApplDate').$inipay->GetResult('ApplTime')); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 175 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\taxsave\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6",$inipay->GetResult('ApplDate').$inipay->GetResult('ApplTime')); ?></td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$paymethod = isset($paymethod) ? preg\_replace('/[^0-9a-z\_\-]/i', '', $paymethod) : '';

**STANDARD: Potentially Unsafe Code - fopen**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

$this->handle = fopen($logfile, "a+");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$this->handle = fopen($logfile, "a+");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($this->handle, $pfx . $key . ":" . $val . "\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($this->handle, $pfx . $data . "\r\n");

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 470 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

mt\_srand(getmypid() \* mt\_rand(1, 999));

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 472 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$this->m\_sTID = $this->m\_REQUEST["pgid"] . $this->m\_REQUEST["mid"] . $datestr\_con . mt\_rand(1000, 9999);

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 484 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$out .= chr(mt\_rand($nullOk ? 0 : 1, $ascii ? 127 : 255 ));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1097 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($fp, $out);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 1152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

$fp = fopen($this->homedir . "/key/pgcert.pem", "r");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fp = fopen($this->homedir . "/key/pgcert.pem", "r");

**STANDARD: Potentially Unsafe Code - fopen**

Line: 1177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

$fp = fopen($f\_new, "w");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fp = fopen($f\_new, "w");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($fp, $pgpubkey);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 1191 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

$fp = fopen($this->homedir . "/key/mkey/mcert.pem", "r");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1191 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fp = fopen($this->homedir . "/key/mkey/mcert.pem", "r");

**STANDARD: Potentially Unsafe Code - fopen**

Line: 1193 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

$fp = fopen($this->homedir . "/key/" . $this->mid . "/mcert.pem", "r");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1193 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fp = fopen($this->homedir . "/key/" . $this->mid . "/mcert.pem", "r");

**STANDARD: Potentially Unsafe Code - fopen**

Line: 1226 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

$fp = fopen($this->homedir . "/key/mkey/mpriv.pem", "r");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1226 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fp = fopen($this->homedir . "/key/mkey/mpriv.pem", "r");

**STANDARD: Potentially Unsafe Code - fopen**

Line: 1228 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

$fp = fopen($this->homedir . "/key/" . $this->mid . "/mpriv.pem", "r");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 1228 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INICls.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fp = fopen($this->homedir . "/key/" . $this->mid . "/mpriv.pem", "r");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 228 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INIXml.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$content = implode("", file($file));

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 3117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\INIXml.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<b>phpXML error:</b> " . $message;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 455 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\inicis\libs\JSON.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace(array(

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\inicis\_kk\_return.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$orderNumber = isset($\_POST['orderNumber']) ? preg\_replace("/[ #\&\+%@=\/\\\:;,\.'\"\^`~|\!\?\\*$#<>()\[\]\{\}]/i", "", strip\_tags($\_POST['orderNumber'])) : 0;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\kakaopay\_cancel.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ini\_oid = preg\_replace('/[^a-z0-9\_\-]/i', '', get\_session('ss\_order\_id'));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\kakaopay\_cancel.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$tno = preg\_replace('/[^a-z0-9\_\-]/i', '', $tno);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\kakaopay\_cancel.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

P\_AUTH\_DT = '".preg\_replace('/[^0-9]/', '', G5\_TIME\_YMDHIS)."' where oid = '$ini\_oid' and P\_TID = '$tno' ";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\kakaopay\_cancel.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

P\_AUTH\_DT = '".preg\_replace('/[^0-9]/', '', G5\_TIME\_YMDHIS)."' ";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\kakaopay\_cancel.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$tmp = sql\_fetch("select \* from `{$g5['g5\_shop\_order\_table']}` where od\_tno = '".trim($\_REQUEST['TID'])."' ");

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\kakaopay\_result.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sql = " select \* from {$g5['g5\_shop\_order\_data\_table']} where od\_id = '".preg\_replace("/\s+/", "", $\_POST['P\_NOTI'])."' ";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\makesignature.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$price = preg\_replace('#[^0-9]#', '', $\_POST['price']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\mobile\_orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_OID" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\mobile\_orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_GOODS" value="<?php echo $goods; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\mobile\_orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_AMT" value="<?php echo $tot\_price; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\mobile\_orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_MID" value="<?php echo $default['de\_kakaopay\_mid']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\mobile\_orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_NEXT\_URL" value="<?php echo $next\_url; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\mobile\_orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_NOTI\_URL" value="<?php echo $noti\_url; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\mobile\_orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_RESERVED" value="<?php echo get\_inicis\_app\_scheme(); ?>bank\_receipt=N&twotrs\_isp=Y&block\_isp=Y<?php echo $useescrow; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\mobile\_orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="DEF\_RESERVED" value="<?php echo get\_inicis\_app\_scheme(); ?>bank\_receipt=N&twotrs\_isp=Y&block\_isp=Y<?php echo $useescrow; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\mobile\_orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="P\_NOTI" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\mobile\_orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_mny" value="<?php echo $tot\_price; ?>" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\mobile\_orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

inicis\_kakaopay\_form.P\_RETURN\_URL.value = "<?php echo $return\_url.$od\_id; ?>";

**MEDIUM: Potentially Unsafe Code - md5**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\mobile\_pay\_approval.php

MD5 Hashing algorithm.

$hash = md5($PAY['P\_TID'].$PAY['P\_MID'].$PAY['P\_AMT']);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\mobile\_pay\_result.php

MD5 Hashing algorithm.

$hash = md5(get\_session('P\_TID').$default['de\_kakaopay\_mid'].get\_session('P\_AMT'));

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mid" value="<?php echo $default['de\_kakaopay\_mid']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="goodname" value="<?php echo isset($goods) ? get\_text($goods) : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="oid" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="price" value="<?php echo $tot\_price; ?>" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="returnUrl" value="<?php echo $returnUrl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="acceptmethod" value="<?php echo $acceptmethod; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="closeUrl" value="<?php echo $closeUrl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="popupUrl" value="<?php echo $popupUrl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="nointerest" value="<?php echo $cardNoInterestQuota ?>" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="quotabase" value="<?php echo $cardQuotaBase ?>" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="SupplyAmt" value="<?php echo ((int)$comm\_tax\_mny + (int)$comm\_free\_mny); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="GoodsVat" value="<?php echo $comm\_vat\_mny; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\pc\_pay\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $httpUtil->errormsg;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\pc\_pay\_result.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$oid = preg\_replace('/[^A-Za-z0-9\-\_]/', '', $resultMap['MOID']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\pc\_pay\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $s;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\pc\_pay\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $httpUtil->errormsg;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 189 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\pc\_pay\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<pre>", $netcancelResultString . "</pre>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 209 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kakaopay\pc\_pay\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $s;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\escrow.register.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ordr\_idxx = isset($ordr\_idxx) ? preg\_replace('/[^a-z0-9\_\-]/i', '', $ordr\_idxx) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\global\_nhn\_kcp\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<script src="<?php echo $g\_conf\_js\_url; ?>"></script>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\global\_nhn\_kcp\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="nhnkcp\_pay\_form" id="nhnkcp\_pay\_form" method="POST" action="<?php echo $order\_action\_url; ?>" style="display:none">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\global\_nhn\_kcp\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="site\_cd" value="<?php echo $default['de\_kcp\_mid']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\global\_nhn\_kcp\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="site\_name" value="<?php echo $g\_conf\_site\_name; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\global\_nhn\_kcp\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="def\_site\_cd" value="<?php echo $default['de\_kcp\_mid']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\global\_nhn\_kcp\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ordr\_idxx" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\global\_nhn\_kcp\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_name" value="<?php echo isset($goods) ? get\_text($goods) : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\global\_nhn\_kcp\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_mny" value="<?php echo $tot\_price; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 186 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\global\_nhn\_kcp\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="pay\_mod" value="<?php echo ($default['de\_escrow\_use']?"O":"N"); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 192 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\global\_nhn\_kcp\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bask\_cntx" value="<?php echo isset($goods\_count) ? ((int) $goods\_count + 1) : 0; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 248 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\global\_nhn\_kcp\_form.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="kcp\_noint" value="<?php echo ($default['de\_card\_noint\_use'] ? '' : 'N'); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\global\_nhn\_kcp\_order.script.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

nhnkcp\_pay\_form.good\_info.value = "<?php echo $good\_info; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<script src="<?php echo $g\_conf\_js\_url; ?>"></script>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="site\_cd" value="<?php echo $default['de\_kcp\_mid']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="site\_name" value="<?php echo $g\_conf\_site\_name; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="def\_site\_cd" value="<?php echo $default['de\_kcp\_mid']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ordr\_idxx" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_name" value="<?php echo $goods; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_mny" value="<?php echo $tot\_price; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="pay\_mod" value="<?php echo ($default['de\_escrow\_use']?"O":"N"); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bask\_cntx" value="<?php echo (int)$goods\_count + 1; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_info" value="<?php echo $good\_info; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="kcp\_noint" value="<?php echo ($default['de\_card\_noint\_use'] ? '' : 'N'); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 193 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_tax\_mny" value="<?php echo $comm\_tax\_mny; ?>"> <!-- 과세금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 194 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_vat\_mny" value="<?php echo $comm\_vat\_mny; ?>"> <!-- 부가세 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_free\_mny" value="<?php echo $comm\_free\_mny; ?>"> <!-- 비과세 금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\orderform.4.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><a href="http://admin.kcp.co.kr/Modules/escrow/kcp\_pop.jsp?site\_cd=<?php echo $default['de\_kcp\_mid']; ?>" class="nhnkcp\_escrow\_popup" data-sitecd="<?php echo $default['de\_kcp\_mid']; ?>" target="\_blank"><img src="<?php echo G5\_SHOP\_URL; ?>/img/marks\_escrow/escrow\_foot.gif" width="290" height="92" border="0" usemap="#Map"></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\orderform.4.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <?php if ($default['de\_card\_use'] || $default['de\_iche\_use']) { echo "결제대행사 : KCP"; } ?> -->

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_ax\_hub.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$tran\_cd = isset($\_POST['tran\_cd']) ? preg\_replace('/[^0-9A-Za-z\_\-\.]/i', '', $\_POST['tran\_cd']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_ax\_hub.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ordr\_idxx = isset($\_POST['ordr\_idxx']) ? preg\_replace('/[^0-9A-Za-z\_\-\.]/i', '', $\_POST['ordr\_idxx']) : '';

**STANDARD: Potentially Unsafe Code - exec**

Line: 292 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_ax\_hub\_lib.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$rt = exec( $exec\_cmd );

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 292 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_ax\_hub\_lib.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

$rt = exec( $exec\_cmd );

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$ordr\_idxx = isset($\_POST["ordr\_idxx"]) ? preg\_replace('/[^0-9A-Za-z\_\-\.]/i', '', $\_POST[ "ordr\_idxx" ]) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 343 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="req\_tx" value="<?php echo $req\_tx; ?>"> <!-- 요청 구분 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 344 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bSucc" value="<?php echo $bSucc; ?>"> <!-- 쇼핑몰 DB 처리 성공 여부 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 346 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="res\_cd" value="<?php echo $res\_cd; ?>"> <!-- 결과 코드 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 347 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="res\_msg" value="<?php echo iconv("cp949", "utf-8", $res\_msg); ?>"> <!-- 결과 메세지 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 348 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ordr\_idxx" value="<?php echo $ordr\_idxx; ?>"> <!-- 주문번호 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 349 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_name" value="<?php echo $good\_name; ?>"> <!-- 상품명 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 350 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="buyr\_name" value="<?php echo $buyr\_name; ?>"> <!-- 주문자명 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 351 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="buyr\_tel1" value="<?php echo $buyr\_tel1; ?>"> <!-- 주문자 전화번호 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 352 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="buyr\_mail" value="<?php echo $buyr\_mail; ?>"> <!-- 주문자 E-mail -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 353 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comment" value="<?php echo $comment; ?>"> <!-- 비고 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 355 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="corp\_type" value="<?php echo $corp\_type; ?>"> <!-- 사업장 구분 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 356 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="corp\_tax\_type" value="<?php echo $corp\_tax\_type; ?>"> <!-- 과세/면세 구분 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 357 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="corp\_tax\_no" value="<?php echo $corp\_tax\_no; ?>"> <!-- 발행 사업자 번호 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 358 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="corp\_nm" value="<?php echo $corp\_nm; ?>"> <!-- 상호 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 359 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="corp\_owner\_nm" value="<?php echo $corp\_owner\_nm; ?>"> <!-- 대표자명 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 360 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="corp\_addr" value="<?php echo $corp\_addr; ?>"> <!-- 사업장주소 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 361 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="corp\_telno" value="<?php echo $corp\_telno; ?>"> <!-- 사업장 대표 연락처 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 363 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="tr\_code" value="<?php echo $tr\_code; ?>"> <!-- 발행용도 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 364 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="id\_info" value="<?php echo $id\_info; ?>"> <!-- 신분확인 ID -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 365 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="amt\_tot" value="<?php echo $amt\_tot; ?>"> <!-- 거래금액 총 합 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 366 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="amt\_sub" value="<?php echo $amt\_sup; ?>"> <!-- 공급가액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 367 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="amt\_svc" value="<?php echo $amt\_svc; ?>"> <!-- 봉사료 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 368 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="amt\_tax" value="<?php echo $amt\_tax; ?>"> <!-- 부가가치세 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 369 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="pay\_type" value="<?php echo $pay\_type; ?>"> <!-- 결제 서비스 구분 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 370 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="pay\_trade\_no" value="<?php echo $pay\_trade\_no; ?>"> <!-- 결제 거래번호 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 372 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mod\_type" value="<?php echo $mod\_type; ?>"> <!-- 변경 타입 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 373 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mod\_value" value="<?php echo $mod\_value; ?>"> <!-- 변경 요청 거래번호 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 374 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mod\_gubn" value="<?php echo $mod\_gubn; ?>"> <!-- 변경 요청 거래번호 구분 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 375 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mod\_mny" value="<?php echo $mod\_mny; ?>"> <!-- 변경 요청 금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 376 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="rem\_mny" value="<?php echo $rem\_mny; ?>"> <!-- 변경처리 이전 금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 378 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cash\_no" value="<?php echo $cash\_no; ?>"> <!-- 현금영수증 거래번호 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 379 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="receipt\_no" value="<?php echo $receipt\_no; ?>"> <!-- 현금영수증 승인번호 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 380 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="app\_time" value="<?php echo $app\_time; ?>"> <!-- 승인시간(YYYYMMDDhhmmss) -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 381 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="reg\_stat" value="<?php echo $reg\_stat; ?>"> <!-- 등록 상태 코드 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 382 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="reg\_desc" value="<?php echo iconv("cp949", "utf-8", $reg\_desc); ?>"> <!-- 등록 상태 설명 -->

**STANDARD: Potentially Unsafe Code - exec**

Line: 288 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub\_lib.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$rt = exec( $exec\_cmd );

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 288 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_hub\_lib.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

$rt = exec( $exec\_cmd );

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<title>현금영수증발급 <?php echo $req\_tx\_name; ?> | <?php echo $config['cf\_title']; ?></title>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var receiptWin = "<?php echo G5\_CASH\_RECEIPT\_URL.$default['de\_kcp\_mid'].'&orderid='.$ordr\_idxx.'&bill\_yn=Y&authno='; ?>"+auth\_no;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title">현금영수증 <?php echo $req\_tx\_name; ?> - KCP Online Payment System</h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $res\_cd; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $res\_msg; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $cash\_no; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $receipt\_no; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $reg\_stat; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $reg\_desc; ?></td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

<td><?php echo preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6",$app\_time); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6",$app\_time); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" name="receiptView" class="btn\_frmline" onClick="javascript:receiptView('<?php echo $receipt\_no; ?>')">영수증 확인</button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 172 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $res\_cd; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $res\_msg; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $res\_cd; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 191 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $res\_msg; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 219 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $res\_cd; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 223 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $res\_msg; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 227 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $cash\_no; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 231 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $receipt\_no; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 235 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $reg\_stat; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 239 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $reg\_desc; ?></td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 243 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

<td><?php echo preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 243 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6", $app\_time); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 248 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="button" name="receiptView" value="영수증 확인" class="box" onClick="javascript:receiptView('<?php echo $receipt\_no; ?>')">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 259 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $res\_cd; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 263 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\pp\_cli\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $res\_msg; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

form.ordr\_idxx.value = "<?php echo $od\_id; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

form.amt\_tot.value = "<?php echo $amt\_tot; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

form.amt\_sup.value = "<?php echo $amt\_sup; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

form.amt\_svc.value = "<?php echo $amt\_svc; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

form.amt\_tax.value = "<?php echo $amt\_tax; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title']; ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od\_id; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $goods\_name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od\_name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od\_email; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od\_tel; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="tx" value="<?php echo $tx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_name" value="<?php echo addslashes($goods\_name); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="buyr\_name" value="<?php echo $od\_name; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="buyr\_mail" value="<?php echo $od\_email; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="buyr\_tel1" value="<?php echo $od\_tel; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="trad\_time" value="<?php echo $trad\_time; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 182 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $trad\_time; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 206 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($amt\_tot); ?>원</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 210 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($amt\_sup); ?>원<!-- ((거래금액 총합 \* 10) / 11) --></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 214 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($amt\_svc); ?>원</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 218 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\kcp\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($amt\_tax); ?>원<!-- 거래금액 총합 - 공급가액 - 봉사료 --></td>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\escrow.register.php

MD5 Hashing algorithm.

$hashdata = md5($mid.$oid.$dlvdate.$dlvcompcode.$dlvno.$mertkey);

**STANDARD: Potentially Unsafe Code - fopen**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\escrow.register.php

$fp = @fopen($str\_url,"r");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\escrow.register.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$fp = @fopen($str\_url,"r");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<script language="javascript" src="<?php echo (isset($\_SERVER['HTTPS']) && $\_SERVER['HTTPS']=='on') ? 'https' : 'http'; ?>:

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var LGD\_window\_type = "<?php echo $LGD\_WINDOW\_TYPE; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

lgdwin = openXpay(frm, '<?php echo $CST\_PLATFORM; ?>', LGD\_window\_type, null, "", "");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.getElementById("forderform").action = "<?php echo $order\_action\_url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.getElementById("forderform").action = "<?php echo $order\_action\_url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="CST\_PLATFORM" id="CST\_PLATFORM" value="<?php echo $CST\_PLATFORM; ?>"> <!-- 테스트, 서비스 구분 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="CST\_MID" id="CST\_MID" value="<?php echo $CST\_MID; ?>"> <!-- 상점아이디 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="LGD\_MID" id="LGD\_MID" value="<?php echo $LGD\_MID; ?>"> <!-- 상점아이디 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="LGD\_OID" id="LGD\_OID" value="<?php echo $od\_id; ?>"> <!-- 주문번호 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="LGD\_PRODUCTINFO" id="LGD\_PRODUCTINFO" value="<?php echo $goods; ?>"> <!-- 상품정보 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="LGD\_CUSTOM\_SKIN" id="LGD\_CUSTOM\_SKIN" value="<?php echo $LGD\_CUSTOM\_SKIN; ?>"> <!-- 결제창 SKIN -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="LGD\_WINDOW\_VER" id="LGD\_WINDOW\_VER" value="<?php echo $LGD\_WINDOW\_VER; ?>"> <!-- 결제창버전정보 (삭제하지 마세요) -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="LGD\_CUSTOM\_PROCESSTYPE" id="LGD\_CUSTOM\_PROCESSTYPE" value="<?php echo $LGD\_CUSTOM\_PROCESSTYPE; ?>"> <!-- 트랜잭션 처리방식 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="LGD\_TIMESTAMP" id="LGD\_TIMESTAMP" value="<?php echo $LGD\_TIMESTAMP; ?>"> <!-- 타임스탬프 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="LGD\_VERSION" id="LGD\_VERSION" value="<?php echo $LGD\_VERSION; ?>"> <!-- 버전정보 (삭제하지 마세요) -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="LGD\_TAXFREEAMOUNT" id="LGD\_TAXFREEAMOUNT" value="<?php echo $comm\_free\_mny; ?>"> <!-- 결제금액 중 면세금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="LGD\_BUYERIP" id="LGD\_BUYERIP" value="<?php echo $LGD\_BUYERIP; ?>"> <!-- 구매자IP -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="LGD\_BUYERID" id="LGD\_BUYERID" value="<?php echo $LGD\_BUYERID; ?>"> <!-- 구매자ID -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="LGD\_CUSTOM\_USABLEPAY" id="LGD\_CUSTOM\_USABLEPAY" value="<?php echo $LGD\_CUSTOM\_USABLEPAY; ?>"> <!-- 결제가능수단 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="LGD\_CASNOTEURL" id="LGD\_CASNOTEURL" value="<?php echo $LGD\_CASNOTEURL ?>"> <!-- 가상계좌 NOTEURL -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="LGD\_RETURNURL" id="LGD\_RETURNURL" value="<?php echo $LGD\_RETURNURL; ?>"> <!-- 응답수신페이지 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="good\_mny" value="<?php echo $tot\_price; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_tax\_mny" value="<?php echo $comm\_tax\_mny; ?>"> <!-- 과세금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_vat\_mny" value="<?php echo $comm\_vat\_mny; ?>"> <!-- 부가세 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\orderform.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comm\_free\_mny" value="<?php echo $comm\_free\_mny; ?>"> <!-- 비과세 금액 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\returnurl.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "LGD\_RESPCODE:" . $LGD\_RESPCODE . " ,LGD\_RESPMSG:" . $LGD\_RESPMSG;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\returnurl.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<input type='hidden' name='$key' id='$key' value='$value'>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title']; ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od\_id; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $goods\_name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od\_name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od\_email; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od\_tel; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="tx" value="<?php echo $tx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_id" value="<?php echo $od\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $trad\_time; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($amt\_tot); ?>원</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($amt\_sup); ?>원<!-- ((거래금액 총합 \* 10) / 11) --></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($amt\_svc); ?>원</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_form.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($amt\_tax); ?>원<!-- 거래금액 총합 - 공급가액 - 봉사료 --></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 225 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $xpay->Response\_Code(); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 229 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $xpay->Response\_Msg(); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 233 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $xpay->Response("LGD\_TID",0); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 237 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $xpay->Response("LGD\_CASHRECEIPTNUM",0); ?></td>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 241 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_result.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

<td><?php echo preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6",$xpay->Response("LGD\_RESPDATE",0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 241 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo preg\_replace("/([0-9]{4})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})([0-9]{2})/", "\\1-\\2-\\3 \\4:\\5:\\6",$xpay->Response("LGD\_RESPDATE",0)); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 246 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\taxsave\_result.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" name="receiptView" class="btn\_frmline" onClick="javascript:showCashReceipts('<?php echo $LGD\_MID; ?>','<?php echo $LGD\_OID; ?>','<?php echo $od\_casseqno; ?>','<?php echo $trade\_type; ?>','<?php echo $CST\_PLATFORM; ?>');">영수증 확인</button>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\lg\xpay\_request.php

MD5 Hashing algorithm.

$LGD\_HASHDATA = md5($LGD\_MID.$LGD\_OID.$LGD\_AMOUNT.$LGD\_TIMESTAMP.$xpay->config[$LGD\_MID]);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\couponmail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<title><?php echo $config['cf\_title']; ?> - 쿠폰발행알림 메일</title>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\couponmail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $config['cf\_title'];?> - 쿠폰발행알림 메일

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\couponmail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p style="<?php echo $cont\_st; ?>"><b><?php echo $mb\_name; ?></b> 님께 발행된 쿠폰입니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\couponmail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p style="<?php echo $cont\_st; ?>"><?php echo $contents; ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\couponmail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_URL; ?>" target="\_blank" style="<?php echo $ft\_a\_st; ?>"><?php echo $config['cf\_title']; ?> 바로가기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\itemrecommend.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<title><?php echo $config['cf\_title']; ?> - <?php echo $from\_name; ?> 의 상품 추천 메일</title>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\itemrecommend.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $config['cf\_title'];?> - 상품 추천 메일

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\itemrecommend.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p style="<?php echo $cont\_st; ?>"><b><?php echo $from\_name; ?></b> 님께서 추천하신 상품입니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\itemrecommend.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo shop\_item\_url($it\_id); ?>" target="\_blank" style="display:inline-block;margin:0 0 10px"><?php echo $it\_mimg; ?></a><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\itemrecommend.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $it\_name; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\itemrecommend.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\itemrecommend.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $subject; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\itemrecommend.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p style="<?php echo $cont\_st; ?>"><?php echo $content; ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\itemrecommend.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo shop\_item\_url($it\_id); ?>" target="\_blank" style="<?php echo $ft\_a\_st; ?>">상품 자세히 보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 5 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<title><?php echo $config['cf\_title'];?> - 주문내역 처리 안내</title>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $config['cf\_title'];?> - 주문내역 처리 안내

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<table style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption style="<?php echo $caption\_st; ?>">주문상품 확인</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col" style="<?php echo $th\_st; ?>">품명</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col" style="<?php echo $th\_st; ?>">옵션</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col" style="<?php echo $th\_st; ?>">상태</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><a href="<?php echo shop\_item\_url($cart\_list[$h]['it\_id']); ?>" target="\_blank" style="text-decoration:none"><?php echo $cart\_list[$h]['it\_name']; ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>;text-align:center"><?php echo $cart\_list[$h]['it\_opt']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>;text-align:center"><?php echo $cart\_list[$h]['ct\_status']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<table style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption style="<?php echo $caption\_st; ?>">신용카드 결제 확인</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">승인일시</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $card\_list['od\_receipt\_time']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">승인금액</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $card\_list['od\_receipt\_price']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<table style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption style="<?php echo $caption\_st; ?>">무통장 입금 확인 완료</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">확인일시</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $bank\_list['od\_receipt\_time']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">입금액</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $bank\_list['od\_receipt\_price']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">입금자명</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $bank\_list['od\_deposit\_name']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<table style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption style="<?php echo $caption\_st; ?>">포인트 결제 확인</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">확인일시</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $point\_list['od\_time']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">포인트</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $point\_list['od\_receipt\_point']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<table style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption style="<?php echo $caption\_st; ?>">배송 안내</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">배송회사</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $delivery\_list['dl\_company']; ?> <?php echo $delivery\_list['dl\_inquiry']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">운송장번호</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $delivery\_list['od\_invoice']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">배송일시</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $delivery\_list['od\_invoice\_time']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $addmemo; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\ordermail.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_SHOP\_URL ?>" target="\_blank" style="<?php echo $ft\_a\_st; ?>"><?php echo $config['cf\_title'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<title><?php echo $config['cf\_title']; ?> - 주문 알림 메일</title>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $config['cf\_title'];?> - 주문이 접수되었습니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong>주문번호 <?php echo $od\_id; ?></strong><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<table style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption style="<?php echo $caption\_st; ?>"> 주문 내역</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">상품명</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><a href="<?php echo shop\_item\_url($list[$i]['it\_id']); ?>" target="\_blank" style="text-decoration:none"><span style="display:inline-block;vertical-align:middle"><?php echo $list[$i]['it\_simg']; ?></span> <?php echo $list[$i]['it\_name']; ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">판매가격</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_price($list[$i]['ct\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">선택옵션 </th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $list[$i]['it\_opt']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">소계</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_price($list[$i]['stotal\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">포인트</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_point($list[$i]['stotal\_point']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">배송비</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_price($od\_send\_cost); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">추가배송비</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_price($od\_send\_cost2); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">주문합계</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_price($ttotal\_price); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">포인트합계</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_point($ttotal\_point); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<table style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption style="<?php echo $caption\_st; ?>">결제정보</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">포인트 입금액</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_point($od\_receipt\_point); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">신용카드 입금액</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_price($od\_receipt\_price); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>"><?php echo $od\_settle\_case; ?> 입금액</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_price($od\_receipt\_price); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">계좌번호</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_bank\_account; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">입금자 이름</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_deposit\_name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="2" style="<?php echo $empty\_st; ?>">결제정보가 없습니다.</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<table style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption style="<?php echo $caption\_st; ?>">주문하신 분 정보</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">이름</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">전화번호</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_tel; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">핸드폰</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_hp; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">주소</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo sprintf("(%s%s)", $od\_zip1, $od\_zip2).' '.print\_address($od\_addr1, $od\_addr2, $od\_addr3, $od\_addr\_jibeon); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">희망배송일</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_hope\_date;?> (<?php echo get\_yoil($od\_hope\_date);?>)</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<table style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption style="<?php echo $caption\_st; ?>">배송지 정보</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">이 름</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 172 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_b\_name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 175 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">전화번호</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_b\_tel; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">핸드폰</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_b\_hp; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 183 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">주소</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 184 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo sprintf("(%s%s)", $od\_b\_zip1, $od\_b\_zip2).' '.print\_address($od\_b\_addr1, $od\_b\_addr2, $od\_b\_addr3, $od\_b\_addr\_jibeon); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">전하실 말씀</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_memo; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 193 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate1.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_ADMIN\_URL.'/shop\_admin/orderform.php?od\_id='.$od\_id; ?>" target="\_blank" style="<?php echo $ft\_a\_st; ?>">관리자 모드에서 주문 확인</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<title><?php echo $config['cf\_title']; ?> - 주문 알림 메일</title>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $config['cf\_title'];?> - 주문이 접수되었습니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong>주문번호 <?php echo $od\_id; ?></strong><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<table style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption style="<?php echo $caption\_st; ?>"> 주문 내역</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">상품명</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><a href="<?php echo shop\_item\_url($list[$i]['it\_id']); ?>" target="\_blank" style="text-decoration:none"><span style="display:inline-block;vertical-align:middle"><?php echo $list[$i]['it\_simg']; ?></span> <?php echo $list[$i]['it\_name']; ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">판매가격</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_price($list[$i]['ct\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">선택옵션 </th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $list[$i]['it\_opt']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">소계</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_price($list[$i]['stotal\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">포인트</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_point($list[$i]['stotal\_point']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">배송비</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_price($od\_send\_cost); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">추가배송비</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_price($od\_send\_cost2); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">주문합계</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_price($ttotal\_price); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">포인트합계</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_point($ttotal\_point); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<table style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption style="<?php echo $caption\_st; ?>">결제정보</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">포인트 입금액</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_point($od\_receipt\_point); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">신용카드 입금액</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_price($od\_receipt\_price); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>"><?php echo $od\_settle\_case; ?> 입금액</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_price($od\_receipt\_price); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">계좌번호</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_bank\_account; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">입금자 이름</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_deposit\_name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="2" style="<?php echo $empty\_st; ?>">결제정보가 없습니다.</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<table style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption style="<?php echo $caption\_st; ?>">주문하신 분 정보</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">이름</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">전화번호</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_tel; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">핸드폰</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_hp; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">주소</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo sprintf("(%s%s)", $od\_zip1, $od\_zip2).' '.print\_address($od\_addr1, $od\_addr2, $od\_addr3, $od\_addr\_jibeon); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">희망배송일</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_hope\_date;?> (<?php echo get\_yoil($od\_hope\_date);?>)</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<table style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption style="<?php echo $caption\_st; ?>">배송지 정보</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">이 름</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 172 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_b\_name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 175 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">전화번호</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_b\_tel; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">핸드폰</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_b\_hp; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 183 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">주소</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 184 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo sprintf("(%s%s)", $od\_b\_zip1, $od\_b\_zip2).' '.print\_address($od\_b\_addr1, $od\_b\_addr2, $od\_b\_addr3, $od\_b\_addr\_jibeon); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">전하실 말씀</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_memo; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 193 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p style="<?php echo $cont\_st; ?>">배송지를 변경하실 고객님은 <b><?php echo $default['de\_admin\_company\_tel']; ?></b>로 연락주시기 바랍니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate2.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_SHOP\_URL.'/orderinquiry.php'; ?>" target="\_blank" style="<?php echo $ft\_a\_st; ?>">주문상세내역 확인</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<title><?php echo $config['cf\_title']; ?> - 주문 알림 메일</title>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $config['cf\_title'];?> - 주문이 접수되었습니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong>주문번호 <?php echo $od\_id; ?></strong><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<table style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption style="<?php echo $caption\_st; ?>"> 주문 내역</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">상품명</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><a href="<?php echo shop\_item\_url($list[$i]['it\_id']); ?>" target="\_blank" style="text-decoration:none"><span style="display:inline-block;vertical-align:middle"><?php echo $list[$i]['it\_simg']; ?></span> <?php echo $list[$i]['it\_name']; ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">판매가격</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo display\_price($list[$i]['ct\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">선택옵션 </th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $list[$i]['it\_opt']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<table style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption style="<?php echo $caption\_st; ?>">주문하신 분 정보</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">이름</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">전화번호</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_tel; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">핸드폰</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_hp; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">주소</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo sprintf("(%s%s)", $od\_zip1, $od\_zip2).' '.print\_address($od\_addr1, $od\_addr2, $od\_addr3, $od\_addr\_jibeon); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">희망배송일</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_hope\_date;?> (<?php echo get\_yoil($od\_hope\_date);?>)</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<table style="<?php echo $cont\_st; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption style="<?php echo $caption\_st; ?>">배송지 정보</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">이 름</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_b\_name; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">전화번호</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_b\_tel; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">핸드폰</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_b\_hp; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">주소</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo sprintf("(%s%s)", $od\_b\_zip1, $od\_b\_zip2).' '.print\_address($od\_b\_addr1, $od\_b\_addr2, $od\_b\_addr3, $od\_b\_addr\_jibeon); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row" style="<?php echo $th\_st; ?>">전하실 말씀</th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td style="<?php echo $td\_st; ?>"><?php echo $od\_memo; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p style="<?php echo $cont\_st; ?>">이 주문과 관련된 내용은 <b><?php echo $default['de\_admin\_company\_tel']; ?></b>로 연락주시기 바랍니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\mail\orderupdate3.mail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_SHOP\_URL.'/'; ?>" target="\_blank" style="<?php echo $ft\_a\_st; ?>"><?php echo $config['cf\_title']; ?></a>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_item.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$value = preg\_replace("/[^A-Za-z0-9\-\_]/", "", urldecode($value));

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<item id="<?php echo $id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<mall\_pid><![CDATA[<?php echo $it['ec\_mall\_pid']; ?>]]></mall\_pid>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<name><![CDATA[<?php echo $name; ?>]]></name>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<url><?php echo shop\_item\_url($it\_id); ?></url>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<description><![CDATA[<?php echo $description; ?>]]></description>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<image><?php echo $image; ?></image>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<thumb><?php echo $image; ?></thumb>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<price><?php echo $price; ?></price>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<quantity><?php echo $quantity; ?></quantity>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<first id="MJ01"><![CDATA[<?php echo $ca\_name; ?>]]></first>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<second id="ML01"><![CDATA[<?php echo $ca\_name2; ?>]]></second>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<third id="MN01"><![CDATA[<?php echo $ca\_name3; ?>]]></third>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $option; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_item.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $returnInfo; ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_order.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$it\_id = isset($\_POST['it\_id'][$i]) ? preg\_replace($pattern, '', $\_POST['it\_id'][$i]) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_order.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$it\_id = isset($\_POST['it\_id'][$i]) ? preg\_replace($pattern, '', $\_POST['it\_id'][$i]) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_order.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$io\_id = isset($\_POST['io\_id'][$it\_id][$k]) ? preg\_replace(G5\_OPTION\_ID\_FILTER, '', trim(stripslashes($\_POST['io\_id'][$it\_id][$k]))) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 175 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_order.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$io\_id = isset($\_POST['io\_id'][$it\_id][$k]) ? preg\_replace(G5\_OPTION\_ID\_FILTER, '', trim(stripslashes($\_POST['io\_id'][$it\_id][$k]))) : '';

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 247 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_order.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($nc\_sock, $buy\_req\_url."\r\n" );

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 248 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_order.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($nc\_sock, "Host: ".$req\_host.":".$req\_port."\r\n" );

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 249 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_order.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($nc\_sock, "Content-type: application/x-www-form-urlencoded; charset=utf-8\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 250 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_order.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($nc\_sock, "Content-length: ".strlen($query)."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 251 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_order.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($nc\_sock, "Accept: \*

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_wish.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($nc\_sock, "\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_wish.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($nc\_sock, $query."\r\n");

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_wish.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

fwrite($nc\_sock, "\r\n");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_wish.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "$errstr ($errno)<br>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_wish.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="frm" method="get" action="<?php echo $wishUrl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_wish.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="SHOP\_ID" value="<?php echo $default['de\_naverpay\_mid']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\naverpay\naverpay\_wish.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ITEM\_ID" value="<?php echo $itemIdList[$i]; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\daum.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $lt.'tocnt'.$gt.$totcnt.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\daum.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo iconv('utf-8', 'euc-kr', $str);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\daum.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\daum\_summary.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo iconv('utf-8', 'euc-kr', $str);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\daum\_summary.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $content;

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\google\_feed.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

IF( SUBSTR(a.ca\_id, 3) != \"\", (SELECT ca\_adult\_use FROM `{$g5['g5\_shop\_category\_table']}` WHERE ca\_id = SUBSTR(a.ca\_id, 3)), 0) AS ca\_adult\_parent1,

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\google\_feed.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

IF( SUBSTR(a.ca\_id, 5) != \"\", (SELECT ca\_adult\_use FROM `{$g5['g5\_shop\_category\_table']}` WHERE ca\_id = SUBSTR(a.ca\_id, 5)), 0) AS ca\_adult\_parent2,

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\google\_feed.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

IF( SUBSTR(a.ca\_id, 7) != \"\", (SELECT ca\_adult\_use FROM `{$g5['g5\_shop\_category\_table']}` WHERE ca\_id = SUBSTR(a.ca\_id, 7)), 0) AS ca\_adult\_parent3,

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\google\_feed.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

IF( SUBSTR(a.ca\_id, 9) != \"\", (SELECT ca\_adult\_use FROM `{$g5['g5\_shop\_category\_table']}` WHERE ca\_id = SUBSTR(a.ca\_id, 9)), 0) AS ca\_adult\_parent4

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\google\_feed.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

FROM `{$g5['g5\_shop\_category\_table']}` AS a";

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\google\_feed.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

$sql =" SELECT a.\*, IFNULL((SELECT MAX(`io\_stock\_qty`) FROM `{$g5['g5\_shop\_item\_option\_table']}` WHERE `it\_id` = a.`it\_id` GROUP BY `it\_id`), a.`it\_stock\_qty`) AS in\_stock

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\google\_feed.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

FROM `{$g5['g5\_shop\_item\_table']}` as a

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\google\_feed.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $xml->asXML();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\naver.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "id{$tab}title{$tab}price\_pc{$tab}link{$tab}image\_link{$tab}category\_name1{$tab}category\_name2{$tab}category\_name3{$tab}category\_name4{$tab}brand{$tab}maker{$tab}origin{$tab}point{$tab}review\_count{$tab}shipping{$tab}class{$tab}update\_time";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\naver.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "\n{$row['it\_id']}{$tab}{$row['it\_name']}{$tab}{$row['it\_price']}{$tab}{$item\_link}{$tab}{$img\_url}{$tab}{$cate1}{$tab}{$cate2}{$tab}{$cate3}{$tab}{$cate4}{$tab}{$row['it\_brand']}{$tab}{$row['it\_maker']}{$tab}{$row['it\_origin']}{$tab}{$it\_point}{$tab}{$review\_count}{$tab}{$delivery}{$tab}{$class}{$tab}{$row['it\_update\_time']}";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\naver.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\naver\_summary.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "id{$tab}title{$tab}price\_pc{$tab}link{$tab}image\_link{$tab}category\_name1{$tab}category\_name2{$tab}category\_name3{$tab}category\_name4{$tab}model\_number{$tab}brand{$tab}maker{$tab}origin{$tab}point{$tab}shipping{$tab}class{$tab}update\_time";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\naver\_summary.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "\n{$row['it\_id']}{$tab}{$row['it\_name']}{$tab}{$row['it\_price']}{$tab}{$item\_link}{$tab}{$img\_url}{$tab}{$cate1}{$tab}{$cate2}{$tab}{$cate3}{$tab}{$cate4}{$tab}{$row['it\_model']}{$tab}{$row['it\_brand']}{$tab}{$row['it\_maker']}{$tab}{$row['it\_origin']}{$tab}{$it\_point}{$tab}{$delivery}{$tab}{$class}{$tab}{$row['it\_update\_time']}";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\shop\price\naver\_summary.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="bo\_list" style="width:<?php echo $width; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $board['bo\_subject'] ?> 카테고리</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>Total <?php echo number\_format($total\_count) ?>건</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $page ?> 페이지

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($admin\_href) { ?><li><a href="<?php echo $admin\_href ?>" class="btn\_admin btn" title="관리자"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($rss\_href) { ?><li><a href="<?php echo $rss\_href ?>" class="btn\_b01 btn" title="RSS"><i class="fa fa-rss" aria-hidden="true"></i><span class="sound\_only">RSS</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b01 btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $board['bo\_subject'] ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><?php echo subject\_sort\_link('wr\_hit', $qstr2, 1) ?>조회 </a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_good) { ?><th scope="col"><?php echo subject\_sort\_link('wr\_good', $qstr2, 1) ?>추천 </a></th><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_nogood) { ?><th scope="col"><?php echo subject\_sort\_link('wr\_nogood', $qstr2, 1) ?>비추천 </a></th><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><?php echo subject\_sort\_link('wr\_datetime', $qstr2, 1) ?>날짜 </a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php if ($list[$i]['is\_notice']) echo "bo\_notice"; ?> <?php echo $lt\_class ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_wr\_id[]" value="<?php echo $list[$i]['wr\_id'] ?>" id="chk\_wr\_id\_<?php echo $i ?>" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_wr\_id\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<b class="sound\_only"><?php echo $list[$i]['subject'] ?></b>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['num'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_subject" style="padding-left:<?php echo $list[$i]['reply'] ? (strlen($list[$i]['wr\_reply'])\*10) : '0'; ?>px">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['ca\_name\_href'] ?>" class="bo\_cate\_link"><?php echo $list[$i]['ca\_name'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['href'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['icon\_reply'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_secret'])) echo rtrim($list[$i]['icon\_secret']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['subject'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_hot'])) echo rtrim($list[$i]['icon\_hot']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_file'])) echo rtrim($list[$i]['icon\_file']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_link'])) echo rtrim($list[$i]['icon\_link']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['comment\_cnt']) { ?><span class="sound\_only">댓글</span><span class="cnt\_cmt"><?php echo $list[$i]['wr\_comment']; ?></span><span class="sound\_only">개</span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_name sv\_use"><?php echo $list[$i]['name'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $list[$i]['wr\_hit'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_good) { ?><td class="td\_num"><?php echo $list[$i]['wr\_good'] ?></td><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_nogood) { ?><td class="td\_num"><?php echo $list[$i]['wr\_nogood'] ?></td><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo $list[$i]['datetime2'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (count($list) == 0) { echo '<tr><td colspan="'.$colspan.'" class="empty\_table">게시물이 없습니다.</td></tr>'; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($admin\_href) { ?><li><a href="<?php echo $admin\_href ?>" class="btn\_admin btn" title="관리자"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($rss\_href) { ?><li><a href="<?php echo $rss\_href ?>" class="btn\_b01 btn" title="RSS"><i class="fa fa-rss" aria-hidden="true"></i><span class="sound\_only">RSS</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b01 btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 184 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_board\_sfl\_select\_options($sfl); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo stripslashes($stx) ?>" required id="stx" class="sch\_input" size="25" maxlength="20" placeholder=" 검색어를 입력해주세요">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="bo\_v" style="width:<?php echo $width; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_cate"><?php echo $view['ca\_name'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo cut\_str(get\_text($view['wr\_subject']), 70);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="pf\_img"><?php echo get\_member\_profile\_img($view['mb\_id']) ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자</span> <strong><?php echo $view['name'] ?><?php if ($is\_ip\_view) { echo "&nbsp;($ip)"; } ?></strong><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">댓글</span><strong><a href="#bo\_vc"> <i class="fa fa-commenting-o" aria-hidden="true"></i> <?php echo number\_format($view['wr\_comment']) ?>건</a></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">조회</span><strong><i class="fa fa-eye" aria-hidden="true"></i> <?php echo number\_format($view['wr\_hit']) ?>회</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="if\_date"><span class="sound\_only">작성일</span><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo date("y-m-d H:i", strtotime($view['wr\_datetime'])) ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $list\_href ?>" class="btn\_b01 btn" title="목록"><i class="fa fa-list" aria-hidden="true"></i><span class="sound\_only">목록</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($reply\_href) { ?><li><a href="<?php echo $reply\_href ?>" class="btn\_b01 btn" title="답변"><i class="fa fa-reply" aria-hidden="true"></i><span class="sound\_only">답변</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b01 btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($update\_href) { ?><li><a href="<?php echo $update\_href ?>">수정<i class="fa fa-pencil-square-o" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($delete\_href) { ?><li><a href="<?php echo $delete\_href ?>" onclick="del(this.href); return false;">삭제<i class="fa fa-trash-o" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($copy\_href) { ?><li><a href="<?php echo $copy\_href ?>" onclick="board\_move(this.href); return false;">복사<i class="fa fa-files-o" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($move\_href) { ?><li><a href="<?php echo $move\_href ?>" onclick="board\_move(this.href); return false;">이동<i class="fa fa-arrows" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($search\_href) { ?><li><a href="<?php echo $search\_href ?>">검색<i class="fa fa-search" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($scrap\_href) { ?><a href="<?php echo $scrap\_href; ?>" target="\_blank" class="btn btn\_b03" onclick="win\_scrap(this.href); return false;"><i class="fa fa-bookmark" aria-hidden="true"></i> 스크랩</a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_file\_thumbnail($view\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="bo\_v\_con"><?php echo get\_view\_thumbnail($view['content']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_signature) { ?><p><?php echo $signature ?></p><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $good\_href.'&amp;'.$qstr ?>" id="good\_button" class="bo\_v\_good"><i class="fa fa-thumbs-o-up" aria-hidden="true"></i><span class="sound\_only">추천</span><strong><?php echo number\_format($view['wr\_good']) ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $nogood\_href.'&amp;'.$qstr ?>" id="nogood\_button" class="bo\_v\_nogood"><i class="fa fa-thumbs-o-down" aria-hidden="true"></i><span class="sound\_only">비추천</span><strong><?php echo number\_format($view['wr\_nogood']) ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($board['bo\_use\_good']) { ?><span class="bo\_v\_good"><i class="fa fa-thumbs-o-up" aria-hidden="true"></i><span class="sound\_only">추천</span><strong><?php echo number\_format($view['wr\_good']) ?></strong></span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($board['bo\_use\_nogood']) { ?><span class="bo\_v\_nogood"><i class="fa fa-thumbs-o-down" aria-hidden="true"></i><span class="sound\_only">비추천</span><strong><?php echo number\_format($view['wr\_nogood']) ?></strong></span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['file'][$i]['href']; ?>" class="view\_file\_download">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $view['file'][$i]['source'] ?></strong> <?php echo $view['file'][$i]['content'] ?> (<?php echo $view['file'][$i]['size'] ?>)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_file\_cnt"><?php echo $view['file'][$i]['download'] ?>회 다운로드 | DATE : <?php echo $view['file'][$i]['datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 194 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['link\_href'][$i] ?>" target="\_blank">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $link ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 198 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_link\_cnt"><?php echo $view['link\_hit'][$i] ?>회 연결</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 211 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($prev\_href) { ?><li class="btn\_prv"><span class="nb\_tit"><i class="fa fa-chevron-up" aria-hidden="true"></i> 이전글</span><a href="<?php echo $prev\_href ?>"><?php echo $prev\_wr\_subject;?></a> <span class="nb\_date"><?php echo str\_replace('-', '.', substr($prev\_wr\_date, '2', '8')); ?></span></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 212 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($next\_href) { ?><li class="btn\_next"><span class="nb\_tit"><i class="fa fa-chevron-down" aria-hidden="true"></i> 다음글</span><a href="<?php echo $next\_href ?>"><?php echo $next\_wr\_subject;?></a> <span class="nb\_date"><?php echo str\_replace('-', '.', substr($next\_wr\_date, '2', '8')); ?></span></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 232 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var msg = "파일을 다운로드 하시면 포인트가 차감(<?php echo number\_format($board['bo\_download\_point']) ?>점)됩니다.\n\n포인트는 게시물당 한번만 차감되며 다음에 다시 다운로드 하셔도 중복하여 차감하지 않습니다.\n\n그래도 다운로드 하시겠습니까?";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_min = parseInt(<?php echo $comment\_min ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_max = parseInt(<?php echo $comment\_max ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" class="cmt\_btn"><span class="total"><b>댓글</b> <?php echo $view['wr\_comment']; ?></span><span class="cmt\_more"></span></button>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$comment = preg\_replace("/\[\<a\s.\*href\=\"(http|https|ftp|mms)\:\/\/([^[:space:]]+)\.(mp3|wma|wmv|asf|asx|mpg|mpeg)\".\*\<\/a\>\]/i", "<script>doc\_write(obj\_movie('$1:

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="c\_<?php echo $comment\_id ?>" <?php if ($cmt\_depth) { ?>style="margin-left:<?php echo $cmt\_depth ?>px;border-top-color:#e0e0e0"<?php } ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="pf\_img"><?php echo get\_member\_profile\_img($list[$i]['mb\_id']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<header style="z-index:<?php echo $cmt\_sv; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo get\_text($list[$i]['wr\_name']); ?>님의 <?php if ($cmt\_depth) { ?><span class="sound\_only">댓글의</span><?php } ?> 댓글</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>(<?php echo $list[$i]['ip']; ?>)</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_vc\_hdinfo"><i class="fa fa-clock-o" aria-hidden="true"></i> <time datetime="<?php echo date('Y-m-d\TH:i:s+09:00', strtotime($list[$i]['datetime'])) ?>"><?php echo $list[$i]['datetime'] ?></time></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (strstr($list[$i]['wr\_option'], "secret")) { ?><img src="<?php echo $board\_skin\_url; ?>/img/icon\_secret.gif" alt="비밀글"><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $comment ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="edit\_<?php echo $comment\_id ?>" class="bo\_vc\_w"></span><!-- 수정 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="reply\_<?php echo $comment\_id ?>" class="bo\_vc\_w"></span><!-- 답변 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" value="<?php echo strstr($list[$i]['wr\_option'],"secret") ?>" id="secret\_comment\_<?php echo $comment\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea id="save\_comment\_<?php echo $comment\_id ?>" style="display:none"><?php echo get\_text($list[$i]['content1'], 0) ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_reply']) { ?><li><a href="<?php echo $c\_reply\_href; ?>" onclick="comment\_box('<?php echo $comment\_id ?>', 'c'); return false;">답변</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_edit']) { ?><li><a href="<?php echo $c\_edit\_href; ?>" onclick="comment\_box('<?php echo $comment\_id ?>', 'cu'); return false;">수정</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_del']) { ?><li><a href="<?php echo $list[$i]['del\_link']; ?>" onclick="return comment\_delete();">삭제</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fviewcomment" id="fviewcomment" action="<?php echo $comment\_action\_url; ?>" onsubmit="return fviewcomment\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>" id="w">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comment\_id" value="<?php echo $c\_id ?>" id="comment\_id">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($comment\_min || $comment\_max) { ?>onkeyup="check\_byte('wr\_content', 'char\_count');"<?php } ?>><?php echo $c\_wr\_content; ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_html; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 261 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($is\_guest) echo chk\_captcha\_js(); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 333 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

"<?php echo G5\_SNS\_URL; ?>/view\_comment\_write.sns.skin.php?bo\_table=<?php echo $bo\_table; ?>",

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="sound\_only"><?php echo $g5['title'] ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fwrite" id="fwrite" action="<?php echo $action\_url ?>" onsubmit="return fwrite\_submit(this);" method="post" enctype="multipart/form-data" autocomplete="off" style="width:<?php echo $width; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_hidden;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_name" value="<?php echo $name ?>" id="wr\_name" required class="frm\_input half\_input required" placeholder="이름">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="password" name="wr\_password" id="wr\_password" <?php echo $password\_required ?> class="frm\_input half\_input <?php echo $password\_required ?>" placeholder="비밀번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_email" value="<?php echo $email ?>" id="wr\_email" class="frm\_input half\_input email " placeholder="이메일">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_homepage" value="<?php echo $homepage ?>" id="wr\_homepage" class="frm\_input half\_input" size="50" placeholder="홈페이지">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_subject" value="<?php echo $subject ?>" id="wr\_subject" required class="frm\_input full\_input required" size="50" maxlength="255" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($editor\_content\_js) echo $editor\_content\_js; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" id="btn\_autosave" class="btn\_frmline">임시 저장된 글 (<span id="autosave\_count"><?php echo $autosave\_count; ?></span>)</button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="wr\_content <?php echo $is\_dhtml\_editor ? $config['cf\_editor'] : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p id="char\_count\_desc">이 게시판은 최소 <strong><?php echo $write\_min; ?></strong>글자 이상, 최대 <strong><?php echo $write\_max; ?></strong>글자 이하까지 글을 쓰실 수 있습니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="wr\_link<?php echo $i ?>"><i class="fa fa-link" aria-hidden="true"></i><span class="sound\_only"> 링크 #<?php echo $i ?></span></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_link<?php echo $i ?>" value="<?php if($w=="u"){ echo $write['wr\_link'.$i]; } ?>" id="wr\_link<?php echo $i ?>" class="frm\_input full\_input" size="50">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bf\_file\_<?php echo $i+1 ?>" class="lb\_icon"><i class="fa fa-folder-open" aria-hidden="true"></i><span class="sound\_only"> 파일 #<?php echo $i+1 ?></span></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="file" name="bf\_file[]" id="bf\_file\_<?php echo $i+1 ?>" title="파일첨부 <?php echo $i+1 ?> : 용량 <?php echo $upload\_max\_filesize ?> 이하만 업로드 가능" class="frm\_file ">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bf\_content[]" value="<?php echo ($w == 'u') ? $file[$i]['bf\_content'] : ''; ?>" title="파일 설명을 입력해주세요." class="full\_input frm\_input" size="50" placeholder="파일 설명을 입력해주세요.">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="bf\_file\_del<?php echo $i ?>" name="bf\_file\_del[<?php echo $i; ?>]" value="1"> <label for="bf\_file\_del<?php echo $i ?>"><?php echo $file[$i]['source'].'('.$file[$i]['size'].')'; ?> 파일 삭제</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_html ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="btn\_cancel btn">취소</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 172 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_min = parseInt(<?php echo $write\_min; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_max = parseInt(<?php echo $write\_max; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 198 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 247 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="bo\_gall" style="width:<?php echo $width; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $board['bo\_subject'] ?> 카테고리</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>Total <?php echo number\_format($total\_count) ?>건</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $page ?> 페이지

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($admin\_href) { ?><li><a href="<?php echo $admin\_href ?>" class="btn\_admin btn" title="관리자"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($rss\_href) { ?><li><a href="<?php echo $rss\_href ?>" class="btn\_b01 btn" title="RSS"><i class="fa fa-rss" aria-hidden="true"></i><span class="sound\_only">RSS</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b01 btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php echo implode(' ', $classes); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_wr\_id[]" value="<?php echo $list[$i]['wr\_id'] ?>" id="chk\_wr\_id\_<?php echo $i ?>" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_wr\_id\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<b class="sound\_only"><?php echo $list[$i]['subject'] ?></b>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['num'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="gall\_img" style="<?php if ($board['bo\_gallery\_height'] > 0) echo 'height:'.$board['bo\_gallery\_height'].'px;max-height:'.$board['bo\_gallery\_height'].'px'; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['href'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="is\_notice" style="<?php echo $line\_height\_style; ?>">공지</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo run\_replace('thumb\_image\_tag', $img\_content, $thumb);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['ca\_name\_href'] ?>" class="bo\_cate\_link"><?php echo $list[$i]['ca\_name'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['href'] ?>" class="bo\_tit">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['subject'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_hot'])) echo rtrim($list[$i]['icon\_hot']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_secret'])) echo rtrim($list[$i]['icon\_secret']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['comment\_cnt']) { ?><span class="sound\_only">댓글</span><span class="cnt\_cmt"><?php echo $list[$i]['wr\_comment']; ?></span><span class="sound\_only">개</span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자 </span><?php echo $list[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="gall\_date"><span class="sound\_only">작성일 </span><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$i]['datetime2'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="gall\_view"><span class="sound\_only">조회 </span><i class="fa fa-eye" aria-hidden="true"></i> <?php echo $list[$i]['wr\_hit'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_good) { ?><span class="sound\_only">추천</span><strong><i class="fa fa-thumbs-o-up" aria-hidden="true"></i> <?php echo $list[$i]['wr\_good'] ?></strong><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 160 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_nogood) { ?><span class="sound\_only">비추천</span><strong><i class="fa fa-thumbs-o-down" aria-hidden="true"></i> <?php echo $list[$i]['wr\_nogood'] ?></strong><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (count($list) == 0) { echo "<li class=\"empty\_list\">게시물이 없습니다.</li>"; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($admin\_href) { ?><li><a href="<?php echo $admin\_href ?>" class="btn\_admin btn" title="관리자"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($rss\_href) { ?><li><a href="<?php echo $rss\_href ?>" class="btn\_b01 btn" title="RSS"><i class="fa fa-rss" aria-hidden="true"></i><span class="sound\_only">RSS</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b01 btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 191 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 192 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 196 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_board\_sfl\_select\_options($sfl); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 200 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo stripslashes($stx) ?>" required id="stx" class="sch\_input" size="25" maxlength="20" placeholder="검색어를 입력해주세요">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="bo\_v" style="width:<?php echo $width; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_cate"><?php echo $view['ca\_name'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo cut\_str(get\_text($view['wr\_subject']), 70);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="pf\_img"><?php echo get\_member\_profile\_img($view['mb\_id']) ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자</span> <strong><?php echo $view['name'] ?><?php if ($is\_ip\_view) { echo "&nbsp;($ip)"; } ?></strong><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">댓글</span><strong><a href="#bo\_vc"> <i class="fa fa-commenting-o" aria-hidden="true"></i> <?php echo number\_format($view['wr\_comment']) ?>건</a></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">조회</span><strong><i class="fa fa-eye" aria-hidden="true"></i> <?php echo number\_format($view['wr\_hit']) ?>회</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="if\_date"><span class="sound\_only">작성일</span><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo date("y-m-d H:i", strtotime($view['wr\_datetime'])) ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $list\_href ?>" class="btn\_b01 btn" title="목록"><i class="fa fa-list" aria-hidden="true"></i><span class="sound\_only">목록</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($reply\_href) { ?><li><a href="<?php echo $reply\_href ?>" class="btn\_b01 btn" title="답변"><i class="fa fa-reply" aria-hidden="true"></i><span class="sound\_only">답변</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b01 btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($update\_href) { ?><li><a href="<?php echo $update\_href ?>">수정<i class="fa fa-pencil-square-o" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($delete\_href) { ?><li><a href="<?php echo $delete\_href ?>" onclick="del(this.href); return false;">삭제<i class="fa fa-trash-o" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($copy\_href) { ?><li><a href="<?php echo $copy\_href ?>" onclick="board\_move(this.href); return false;">복사<i class="fa fa-files-o" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($move\_href) { ?><li><a href="<?php echo $move\_href ?>" onclick="board\_move(this.href); return false;">이동<i class="fa fa-arrows" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($search\_href) { ?><li><a href="<?php echo $search\_href ?>">검색<i class="fa fa-search" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($scrap\_href) { ?><a href="<?php echo $scrap\_href; ?>" target="\_blank" class="btn btn\_b03" onclick="win\_scrap(this.href); return false;"><i class="fa fa-bookmark" aria-hidden="true"></i> 스크랩</a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_file\_thumbnail($view\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="bo\_v\_con"><?php echo get\_view\_thumbnail($view['content']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_signature) { ?><p><?php echo $signature ?></p><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $good\_href.'&amp;'.$qstr ?>" id="good\_button" class="bo\_v\_good"><i class="fa fa-thumbs-o-up" aria-hidden="true"></i><span class="sound\_only">추천</span><strong><?php echo number\_format($view['wr\_good']) ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $nogood\_href.'&amp;'.$qstr ?>" id="nogood\_button" class="bo\_v\_nogood"><i class="fa fa-thumbs-o-down" aria-hidden="true"></i><span class="sound\_only">비추천</span><strong><?php echo number\_format($view['wr\_nogood']) ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($board['bo\_use\_good']) { ?><span class="bo\_v\_good"><i class="fa fa-thumbs-o-up" aria-hidden="true"></i><span class="sound\_only">추천</span><strong><?php echo number\_format($view['wr\_good']) ?></strong></span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($board['bo\_use\_nogood']) { ?><span class="bo\_v\_nogood"><i class="fa fa-thumbs-o-down" aria-hidden="true"></i><span class="sound\_only">비추천</span><strong><?php echo number\_format($view['wr\_nogood']) ?></strong></span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['file'][$i]['href']; ?>" class="view\_file\_download">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $view['file'][$i]['source'] ?></strong> <?php echo $view['file'][$i]['content'] ?> (<?php echo $view['file'][$i]['size'] ?>)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_file\_cnt"><?php echo $view['file'][$i]['download'] ?>회 다운로드 | DATE : <?php echo $view['file'][$i]['datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 194 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['link\_href'][$i] ?>" target="\_blank">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $link ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 198 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_link\_cnt"><?php echo $view['link\_hit'][$i] ?>회 연결</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 211 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($prev\_href) { ?><li class="btn\_prv"><span class="nb\_tit"><i class="fa fa-chevron-up" aria-hidden="true"></i> 이전글</span><a href="<?php echo $prev\_href ?>"><?php echo $prev\_wr\_subject;?></a> <span class="nb\_date"><?php echo str\_replace('-', '.', substr($prev\_wr\_date, '2', '8')); ?></span></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 212 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($next\_href) { ?><li class="btn\_next"><span class="nb\_tit"><i class="fa fa-chevron-down" aria-hidden="true"></i> 다음글</span><a href="<?php echo $next\_href ?>"><?php echo $next\_wr\_subject;?></a> <span class="nb\_date"><?php echo str\_replace('-', '.', substr($next\_wr\_date, '2', '8')); ?></span></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 232 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var msg = "파일을 다운로드 하시면 포인트가 차감(<?php echo number\_format($board['bo\_download\_point']) ?>점)됩니다.\n\n포인트는 게시물당 한번만 차감되며 다음에 다시 다운로드 하셔도 중복하여 차감하지 않습니다.\n\n그래도 다운로드 하시겠습니까?";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_min = parseInt(<?php echo $comment\_min ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_max = parseInt(<?php echo $comment\_max ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" class="cmt\_btn"><span class="total"><b>댓글</b> <?php echo $view['wr\_comment']; ?></span><span class="cmt\_more"></span></button>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$comment = preg\_replace("/\[\<a\s.\*href\=\"(http|https|ftp|mms)\:\/\/([^[:space:]]+)\.(mp3|wma|wmv|asf|asx|mpg|mpeg)\".\*\<\/a\>\]/i", "<script>doc\_write(obj\_movie('$1:

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="c\_<?php echo $comment\_id ?>" <?php if ($cmt\_depth) { ?>style="margin-left:<?php echo $cmt\_depth ?>px;border-top-color:#e0e0e0"<?php } ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="pf\_img"><?php echo get\_member\_profile\_img($list[$i]['mb\_id']) ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<header style="z-index:<?php echo $cmt\_sv; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo get\_text($list[$i]['wr\_name']); ?>님의 <?php if ($cmt\_depth) { ?><span class="sound\_only">댓글의</span><?php } ?> 댓글</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>(<?php echo $list[$i]['ip']; ?>)</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_vc\_hdinfo"><i class="fa fa-clock-o" aria-hidden="true"></i> <time datetime="<?php echo date('Y-m-d\TH:i:s+09:00', strtotime($list[$i]['datetime'])) ?>"><?php echo $list[$i]['datetime'] ?></time></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (strstr($list[$i]['wr\_option'], "secret")) { ?><img src="<?php echo $board\_skin\_url; ?>/img/icon\_secret.gif" alt="비밀글"><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $comment ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="edit\_<?php echo $comment\_id ?>" class="bo\_vc\_w"></span><!-- 수정 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="reply\_<?php echo $comment\_id ?>" class="bo\_vc\_w"></span><!-- 답변 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" value="<?php echo strstr($list[$i]['wr\_option'],"secret") ?>" id="secret\_comment\_<?php echo $comment\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea id="save\_comment\_<?php echo $comment\_id ?>" style="display:none"><?php echo get\_text($list[$i]['content1'], 0) ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_reply']) { ?><li><a href="<?php echo $c\_reply\_href; ?>" onclick="comment\_box('<?php echo $comment\_id ?>', 'c'); return false;">답변</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_edit']) { ?><li><a href="<?php echo $c\_edit\_href; ?>" onclick="comment\_box('<?php echo $comment\_id ?>', 'cu'); return false;">수정</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_del']) { ?><li><a href="<?php echo $list[$i]['del\_link']; ?>" onclick="return comment\_delete();">삭제</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fviewcomment" id="fviewcomment" action="<?php echo $comment\_action\_url; ?>" onsubmit="return fviewcomment\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>" id="w">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comment\_id" value="<?php echo $c\_id ?>" id="comment\_id">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($comment\_min || $comment\_max) { ?>onkeyup="check\_byte('wr\_content', 'char\_count');"<?php } ?>><?php echo $c\_wr\_content; ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_html; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 262 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($is\_guest) echo chk\_captcha\_js(); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 334 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

"<?php echo G5\_SNS\_URL; ?>/view\_comment\_write.sns.skin.php?bo\_table=<?php echo $bo\_table; ?>",

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="sound\_only"><?php echo $g5['title'] ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fwrite" id="fwrite" action="<?php echo $action\_url ?>" onsubmit="return fwrite\_submit(this);" method="post" enctype="multipart/form-data" autocomplete="off" style="width:<?php echo $width; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_hidden;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_name" value="<?php echo $name ?>" id="wr\_name" required class="frm\_input half\_input required" placeholder="이름">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="password" name="wr\_password" id="wr\_password" <?php echo $password\_required ?> class="frm\_input half\_input <?php echo $password\_required ?>" placeholder="비밀번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_email" value="<?php echo $email ?>" id="wr\_email" class="frm\_input half\_input email " placeholder="이메일">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_homepage" value="<?php echo $homepage ?>" id="wr\_homepage" class="frm\_input half\_input" size="50" placeholder="홈페이지">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_subject" value="<?php echo $subject ?>" id="wr\_subject" required class="frm\_input full\_input required" size="50" maxlength="255" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($editor\_content\_js) echo $editor\_content\_js; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" id="btn\_autosave" class="btn\_frmline">임시 저장된 글 (<span id="autosave\_count"><?php echo $autosave\_count; ?></span>)</button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="wr\_content <?php echo $is\_dhtml\_editor ? $config['cf\_editor'] : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p id="char\_count\_desc">이 게시판은 최소 <strong><?php echo $write\_min; ?></strong>글자 이상, 최대 <strong><?php echo $write\_max; ?></strong>글자 이하까지 글을 쓰실 수 있습니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="wr\_link<?php echo $i ?>"><i class="fa fa-link" aria-hidden="true"></i><span class="sound\_only"> 링크 #<?php echo $i ?></span></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_link<?php echo $i ?>" value="<?php if($w=="u"){ echo $write['wr\_link'.$i]; } ?>" id="wr\_link<?php echo $i ?>" class="frm\_input full\_input" size="50">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bf\_file\_<?php echo $i+1 ?>" class="lb\_icon"><i class="fa fa-folder-open" aria-hidden="true"></i><span class="sound\_only"> 파일 #<?php echo $i+1 ?></span></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="file" name="bf\_file[]" id="bf\_file\_<?php echo $i+1 ?>" title="파일첨부 <?php echo $i+1 ?> : 용량 <?php echo $upload\_max\_filesize ?> 이하만 업로드 가능" class="frm\_file ">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bf\_content[]" value="<?php echo ($w == 'u') ? $file[$i]['bf\_content'] : ''; ?>" title="파일 설명을 입력해주세요." class="full\_input frm\_input" size="50" placeholder="파일 설명을 입력해주세요.">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="bf\_file\_del<?php echo $i ?>" name="bf\_file\_del[<?php echo $i; ?>]" value="1"> <label for="bf\_file\_del<?php echo $i ?>"><?php echo $file[$i]['source'].'('.$file[$i]['size'].')'; ?> 파일 삭제</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_html ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="btn\_cancel btn">취소</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_min = parseInt(<?php echo $write\_min; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_max = parseInt(<?php echo $write\_max; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 196 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 245 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\connect\basic\connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $row['total\_cnt'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\connect\basic\current\_connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="crt\_num"><?php echo $list[$i]['num'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\connect\basic\current\_connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="crt\_profile"><?php echo get\_member\_profile\_img($list[$i]['mb\_id']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\connect\basic\current\_connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="crt\_name"><?php echo $list[$i]['name'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\connect\basic\current\_connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="crt\_lct"><?php echo $display\_location ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\content\basic\content.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="ctt" class="ctt\_<?php echo $co\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\content\basic\content.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title']; ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\content\basic\content.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="faq\_himg" class="faq\_img"><img src="'.$himg\_src.'" alt=""></div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="faq\_hhtml">'.conv\_content($fm['fm\_head\_html'], 1).'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fm\_id" value="<?php echo $fm\_id;?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx;?>" required id="stx" class="frm\_input" size="15" maxlength="15">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $category\_href;?>?fm\_id=<?php echo $v['fm\_id'];?>" <?php echo $category\_option;?> ><?php echo $category\_msg.$v['fm\_subject'];?></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="faq\_wrap" class="faq\_<?php echo $fm\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $g5['title']; ?> 목록</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="tit\_bg">Q</span><a href="#none" onclick="return faq\_open(this);"><?php echo conv\_content($v['fa\_subject'], 1); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($v['fa\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($page\_rows, $page, $total\_page, $\_SERVER['SCRIPT\_NAME'].'?'.$qstr.'&amp;page='); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="faq\_thtml">'.conv\_content($fm['fm\_tail\_html'], 1).'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="faq\_timg" class="faq\_img"><img src="'.$timg\_src.'" alt=""></div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="faq\_admin"><a href="'.$admin\_href.'" class="btn\_admin btn" title="FAQ 수정"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">FAQ 수정</span></a></div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="lat\_title"><a href="<?php echo get\_pretty\_url($bo\_table); ?>"><?php echo $bo\_subject ?></a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_secret']) echo "<i class=\"fa fa-lock\" aria-hidden=\"true\"></i><span class=\"sound\_only\">비밀글</span> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".get\_pretty\_url($bo\_table, $list[$i]['wr\_id'])."\"> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strong>".$list[$i]['subject']."</strong>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_hot']) echo "<span class=\"hot\_icon\"><i class=\"fa fa-heart\" aria-hidden=\"true\"></i><span class=\"sound\_only\">인기글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['icon\_reply']." ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_file']) echo " <i class=\"fa fa-download\" aria-hidden=\"true\"></i>" ;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_link']) echo " <i class=\"fa fa-link\" aria-hidden=\"true\"></i>" ;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['comment\_cnt']) echo "

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="lt\_nick"><?php echo $list[$i]['name'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="lt\_date"><?php echo $list[$i]['datetime2'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="lt\_more"><span class="sound\_only"><?php echo $bo\_subject ?></span>더보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><a href="<?php echo get\_pretty\_url($bo\_table); ?>"><?php echo $bo\_subject ?></a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_secret']) echo "<span class=\"lock\_icon\"><i class=\"fa fa-lock\" aria-hidden=\"true\"></i></span> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".get\_pretty\_url($bo\_table, $list[$i]['wr\_id'])."\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strong>".$list[$i]['subject']."</strong>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['comment\_cnt'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="lat\_title"><a href="<?php echo get\_pretty\_url($bo\_table); ?>"><?php echo $bo\_subject ?></a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $wr\_href; ?>" class="lt\_img"><?php echo run\_replace('thumb\_image\_tag', $img\_content, $thumb); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_secret']) echo "<i class=\"fa fa-lock\" aria-hidden=\"true\"></i><span class=\"sound\_only\">비밀글</span> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".$wr\_href."\"> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strong>".$list[$i]['subject']."</strong>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_hot']) echo "<span class=\"hot\_icon\">H<span class=\"sound\_only\">인기글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['comment\_cnt']) echo "

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="lt\_nick"><?php echo $list[$i]['name'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="lt\_date"><?php echo $list[$i]['datetime2'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="lt\_more"><span class="sound\_only"><?php echo $bo\_subject ?></span>더보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="lat\_title"><a href="<?php echo get\_pretty\_url($bo\_table); ?>"><?php echo $bo\_subject ?></a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $img\_link\_html; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_secret']) echo "<i class=\"fa fa-lock\" aria-hidden=\"true\"></i><span class=\"sound\_only\">비밀글</span> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".$wr\_href."\" class=\"pic\_li\_tit\"> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strong>".$list[$i]['subject']."</strong>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_hot']) echo "<span class=\"hot\_icon\">H<span class=\"sound\_only\">인기글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['comment\_cnt']) echo "

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="lt\_nick"><?php echo $list[$i]['name'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="lt\_date"><?php echo $list[$i]['datetime2'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="lt\_more"><span class="sound\_only"><?php echo $bo\_subject ?></span>더보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="lat\_title"><i class="fa fa-list-ul" aria-hidden="true"></i> <a href="<?php echo G5\_BBS\_URL ?>/board.php?bo\_table=<?php echo $bo\_table ?>"><?php echo $bo\_subject ?></a></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".$list[$i]['href']."\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strong>".$list[$i]['subject']."</strong>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['comment\_cnt'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_new']) && $list[$i]['icon\_new']) echo " <span class=\"new\_icon\">NEW</span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\formmail.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $name ?>님께 메일보내기</h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\formmail.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="to" value="<?php echo $email ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\formmail.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fnick" value="<?php echo get\_text($member['mb\_nick']) ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\formmail.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fmail" value="<?php echo $member['mb\_email'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="flogin" action="<?php echo $login\_action\_url ?>" onsubmit="return flogin\_submit(this);" method="post">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="url" value="<?php echo $login\_url ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($default['de\_guest\_privacy'], $config['cf\_editor']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

f.url.value = "<?php echo $url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

f.action = "<?php echo $url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="forderinquiry" method="post" action="<?php echo urldecode($url); ?>" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_id" value="<?php echo $od\_id; ?>" id="od\_id" required class="frm\_input required" size="20" placeholder="주문서번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fcertrefreshform" id="member\_cert\_refresh" action="<?php echo $action\_url ?>" onsubmit="return fcertrefreshform\_submit(this);" method="POST" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cert\_type" value="<?php echo $member['mb\_certify']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $member['mb\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_hp" value="<?php echo $member['mb\_hp']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_name" value="<?php echo $member['mb\_name']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td>생년월일<?php echo (empty($member['mb\_dupinfo']))? ", 휴대폰 번호(아이핀 제외)" : ""; ?>, 암호화된 개인식별부호(CI)</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

certify\_win\_open("<?php echo $cert\_type; ?>", "<?php echo $cert\_url; ?>" + params);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\member\_confirm.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\member\_confirm.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fmemberconfirm" action="<?php echo $url ?>" onsubmit="return fmemberconfirm\_submit(this);" method="post">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\member\_confirm.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $member['mb\_id'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\member\_confirm.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="mb\_confirm\_id"><?php echo $member['mb\_id'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $g5['title'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="win\_total">전체 <?php echo $kind\_title ?>쪽지 <?php echo $total\_count ?>통<br></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php echo $readed; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($list[$i]['mb\_id']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['name']; ?> <span class="memo\_datetime"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$i]['send\_datetime']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['view\_href']; ?>"><?php echo $memo\_preview; ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['del\_href']; ?>" onclick="del(this.href); return false;" class="memo\_del"><i class="fa fa-trash-o" aria-hidden="true"></i> <span class="sound\_only">삭제</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($i==0) { echo '<li class="empty\_table">자료가 없습니다.</li>'; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p class="win\_desc"><i class="fa fa-info-circle" aria-hidden="true"></i> 쪽지 보관일수는 최장 <strong><?php echo $config['cf\_memo\_del'] ?></strong>일 입니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fmemoform" action="<?php echo $memo\_action\_url; ?>" onsubmit="return fmemoform\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="me\_recv\_mb\_id" value="<?php echo $me\_recv\_mb\_id; ?>" id="me\_recv\_mb\_id" required class="frm\_input full\_input required" size="47" placeholder="받는 회원아이디">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<br ><span class="frm\_info">쪽지 보낼때 회원당 <?php echo number\_format($config['cf\_memo\_send\_point']); ?>점의 포인트를 차감합니다.</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="me\_memo" id="me\_memo" required class="required"><?php echo $content ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($mb['mb\_id']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="memo\_view\_nick"><?php echo $nick ?></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="memo\_view\_date"><span class="sound\_only"><?php echo $kind\_date ?>시간</span><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $memo['me\_send\_datetime'] ?></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="memo\_op\_btn list\_btn"><a href="<?php echo $list\_link ?>" class="btn\_b01 btn"><i class="fa fa-list" aria-hidden="true"></i><span class="sound\_only">목록</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="memo\_op\_btn del\_btn"><a href="<?php echo $del\_link; ?>" onclick="del(this.href); return false;" class="memo\_del btn\_b01 btn"><i class="fa fa-trash-o" aria-hidden="true"></i> <span class="sound\_only">삭제</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $prev\_link ?>" class="btn\_left"><i class="fa fa-chevron-left" aria-hidden="true"></i> 이전쪽지</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $next\_link ?>" class="btn\_right">다음쪽지 <i class="fa fa-chevron-right" aria-hidden="true"></i></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($memo['me\_memo'], 0) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($kind == 'recv') { ?><a href="./memo\_form.php?me\_recv\_mb\_id=<?php echo $mb['mb\_id'] ?>&amp;me\_id=<?php echo $memo['me\_id'] ?>" class="reply\_btn">답장</a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fboardpassword" action="<?php echo $action; ?>" method="post">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comment\_id" value="<?php echo $comment\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\password\_lost.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fpasswordlost" action="<?php echo $action\_url ?>" onsubmit="return fpasswordlost\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\password\_lost.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

certify\_win\_open("<?php echo $cert\_type; ?>", "<?php echo $cert\_url; ?>"+params);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\password\_reset.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fpasswordreset" action="<?php echo $action\_url; ?>" onsubmit="return fpasswordreset\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\password\_reset.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_id" id="mb\_id" value="<?php echo $\_POST['mb\_id']; ?>" required class="required frm\_input full\_input" size="30" placeholder="아이디" readonly>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo number\_format($member['mb\_point']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php echo $point\_use\_class; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="point\_tit"><?php echo $po\_content; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="point\_num"><?php if ($point1) echo $point1; else echo $point2; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="point\_date1"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $row['po\_datetime']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="point\_date<?php echo $expr; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

만료 <?php echo substr(str\_replace('-', '', $row['po\_expire\_date']), 2); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php } else echo $row['po\_expire\_date'] == '9999-12-31' ? '&nbsp;' : $row['po\_expire\_date']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $sum\_point1; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $sum\_point2; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, $\_SERVER['SCRIPT\_NAME'].'?'.$qstr.'&amp;page='); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $mb\_nick ?>님의 프로필</h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($mb['mb\_id']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $mb\_nick ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $mb['mb\_level'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($mb['mb\_point']) ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo ($member['mb\_level'] >= $mb['mb\_level']) ? substr($mb['mb\_datetime'],0,10) ." (".number\_format($mb\_reg\_after)." 일)" : "알 수 없음"; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo ($member['mb\_level'] >= $mb['mb\_level']) ? $mb['mb\_today\_login'] : "알 수 없음"; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="3"><a href="<?php echo $mb\_homepage ?>" target="\_blank"><?php echo $mb\_homepage ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo $mb\_profile ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fregister" id="fregister" action="<?php echo $register\_action\_url ?>" onsubmit="return fregister\_submit(this);" method="POST" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea readonly><?php echo get\_text($config['cf\_stipulation']) ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td>아이디, 이름, 비밀번호<?php echo ($config['cf\_cert\_use'])? ", 생년월일, 휴대폰 번호(본인인증 할 때만, 아이핀 제외), 암호화된 개인식별부호(CI)" : ""; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form id="fregisterform" name="fregisterform" action="<?php echo $register\_action\_url ?>" onsubmit="return fregisterform\_submit(this);" method="post" enctype="multipart/form-data" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="agree" value="<?php echo $agree ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="agree2" value="<?php echo $agree2 ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cert\_type" value="<?php echo $member['mb\_certify']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (isset($member['mb\_sex'])) { ?><input type="hidden" name="mb\_sex" value="<?php echo $member['mb\_sex'] ?>"><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_nick\_default" value="<?php echo get\_text($member['mb\_nick']) ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_nick" value="<?php echo get\_text($member['mb\_nick']) ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_id" value="<?php echo $member['mb\_id'] ?>" id="reg\_mb\_id" <?php echo $required ?> <?php echo $readonly ?> class="frm\_input full\_input <?php echo $required ?> <?php echo $readonly ?>" minlength="3" maxlength="20" placeholder="아이디">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="password" name="mb\_password" id="reg\_mb\_password" <?php echo $required ?> class="frm\_input full\_input <?php echo $required ?>" minlength="3" maxlength="20" placeholder="비밀번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="password" name="mb\_password\_re" id="reg\_mb\_password\_re" <?php echo $required ?> class="frm\_input full\_input <?php echo $required ?>" minlength="3" maxlength="20" placeholder="비밀번호 확인">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $mb\_cert; ?> 본인확인</strong><?php if ($member['mb\_adult']) { ?> 및 <strong>성인인증</strong><?php } ?> 완료

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="reg\_mb\_name">이름 (필수)<?php echo $desc\_name ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" id="reg\_mb\_name" name="mb\_name" value="<?php echo get\_text($member['mb\_name']) ?>" <?php echo $required ?> <?php echo $name\_readonly; ?> class="frm\_input full\_input <?php echo $required ?> <?php echo $name\_readonly ?>" size="10" placeholder="이름">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="tooltip">공백없이 한글,영문,숫자만 입력 가능 (한글2자, 영문4자 이상)<br> 닉네임을 바꾸시면 앞으로 <?php echo (int)$config['cf\_nick\_modify'] ?>일 이내에는 변경 할 수 없습니다.</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_nick\_default" value="<?php echo isset($member['mb\_nick'])?get\_text($member['mb\_nick']):''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_nick" value="<?php echo isset($member['mb\_nick'])?get\_text($member['mb\_nick']):''; ?>" id="reg\_mb\_nick" required class="frm\_input required nospace full\_input" size="10" maxlength="20" placeholder="닉네임">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($w=='') { echo "E-mail 로 발송된 내용을 확인한 후 인증하셔야 회원가입이 완료됩니다."; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($w=='u') { echo "E-mail 주소를 변경하시면 다시 인증하셔야 합니다."; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="old\_email" value="<?php echo $member['mb\_email'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_email" value="<?php echo isset($member['mb\_email'])?$member['mb\_email']:''; ?>" id="reg\_mb\_email" required class="frm\_input email full\_input required" size="70" maxlength="100" placeholder="E-mail">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_homepage" value="<?php echo get\_text($member['mb\_homepage']) ?>" id="reg\_mb\_homepage" <?php echo $config['cf\_req\_homepage']?"required":""; ?> class="frm\_input full\_input <?php echo $config['cf\_req\_homepage']?"required":""; ?>" size="70" maxlength="255" placeholder="홈페이지">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_tel" value="<?php echo get\_text($member['mb\_tel']) ?>" id="reg\_mb\_tel" <?php echo $config['cf\_req\_tel']?"required":""; ?> class="frm\_input full\_input <?php echo $config['cf\_req\_tel']?"required":""; ?>" maxlength="20" placeholder="전화번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="reg\_mb\_hp">휴대폰번호<?php if (!empty($hp\_required)) { ?> (필수)<?php } ?><?php echo $desc\_phone ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_hp" value="<?php echo get\_text($member['mb\_hp']) ?>" id="reg\_mb\_hp" <?php echo $hp\_required; ?> <?php echo $hp\_readonly; ?> class="frm\_input full\_input <?php echo $hp\_required; ?> <?php echo $hp\_readonly; ?>" maxlength="20" placeholder="휴대폰번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="old\_mb\_hp" value="<?php echo get\_text($member['mb\_hp']) ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="reg\_mb\_zip" class="sound\_only">우편번호<?php echo $config['cf\_req\_addr']?' (필수)':''; ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_zip" value="<?php echo $member['mb\_zip1'].$member['mb\_zip2']; ?>" id="reg\_mb\_zip" <?php echo $config['cf\_req\_addr']?"required":""; ?> class="frm\_input twopart\_input <?php echo $config['cf\_req\_addr']?"required":""; ?>" size="5" maxlength="6" placeholder="우편번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_addr1" value="<?php echo get\_text($member['mb\_addr1']) ?>" id="reg\_mb\_addr1" <?php echo $config['cf\_req\_addr']?"required":""; ?> class="frm\_input frm\_address full\_input <?php echo $config['cf\_req\_addr']?"required":""; ?>" size="50" placeholder="기본주소">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="reg\_mb\_addr1" class="sound\_only">기본주소<?php echo $config['cf\_req\_addr']?' (필수)':''; ?></label><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_addr2" value="<?php echo get\_text($member['mb\_addr2']) ?>" id="reg\_mb\_addr2" class="frm\_input frm\_address full\_input" size="50" placeholder="상세주소">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_addr3" value="<?php echo get\_text($member['mb\_addr3']) ?>" id="reg\_mb\_addr3" class="frm\_input frm\_address full\_input" size="50" readonly="readonly" placeholder="참고항목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_addr\_jibeon" value="<?php echo get\_text($member['mb\_addr\_jibeon']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="mb\_signature" id="reg\_mb\_signature" <?php echo $config['cf\_req\_signature']?"required":""; ?> class="<?php echo $config['cf\_req\_signature']?"required":""; ?>" placeholder="서명"><?php echo $member['mb\_signature'] ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="mb\_profile" id="reg\_mb\_profile" <?php echo $config['cf\_req\_profile']?"required":""; ?> class="<?php echo $config['cf\_req\_profile']?"required":""; ?>" placeholder="자기소개"><?php echo $member['mb\_profile'] ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 196 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="tooltip">이미지 크기는 가로 <?php echo $config['cf\_member\_icon\_width'] ?>픽셀, 세로 <?php echo $config['cf\_member\_icon\_height'] ?>픽셀 이하로 해주세요.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 197 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

gif, jpg, png파일만 가능하며 용량 <?php echo number\_format($config['cf\_member\_icon\_size']) ?>바이트 이하만 등록됩니다.</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 202 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<img src="<?php echo $mb\_icon\_url ?>" alt="회원아이콘">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 215 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="tooltip">이미지 크기는 가로 <?php echo $config['cf\_member\_img\_width'] ?>픽셀, 세로 <?php echo $config['cf\_member\_img\_height'] ?>픽셀 이하로 해주세요.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 216 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

gif, jpg, png파일만 가능하며 용량 <?php echo number\_format($config['cf\_member\_img\_size']) ?>바이트 이하만 등록됩니다.</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 221 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<img src="<?php echo $mb\_img\_url ?>" alt="회원이미지">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 230 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="mb\_mailling" value="1" id="reg\_mb\_mailling" <?php echo ($w=='' || $member['mb\_mailling'])?'checked':''; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 240 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="mb\_sms" value="1" id="reg\_mb\_sms" <?php echo ($w=='' || $member['mb\_sms'])?'checked':''; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 251 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="mb\_open" value="1" id="reg\_mb\_open" <?php echo ($w=='' || $member['mb\_open'])?'checked':''; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 259 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

정보공개를 바꾸시면 앞으로 <?php echo (int)$config['cf\_open\_modify'] ?>일 이내에는 변경이 안됩니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 261 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_open\_default" value="<?php echo $member['mb\_open'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 266 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_open" value="<?php echo $member['mb\_open'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 269 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

정보공개는 수정후 <?php echo (int)$config['cf\_open\_modify'] ?>일 이내, <?php echo date("Y년 m월 j일", isset($member['mb\_open\_date']) ? strtotime("{$member['mb\_open\_date']} 00:00:00")+$config['cf\_open\_modify']\*86400:G5\_SERVER\_TIME+$config['cf\_open\_modify']\*86400); ?> 까지는 변경이 안됩니다.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 299 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="submit" id="btn\_submit" class="btn\_submit" accesskey="s"><?php echo $w==''?'회원가입':'정보수정'; ?></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 362 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

certify\_win\_open("<?php echo $cert\_type; ?>", "<?php echo $cert\_url; ?>"+params);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form\_update.tail.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$receive\_number = preg\_replace("/[^0-9]/", "", $mb\_hp);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_form\_update.tail.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace("/[^0-9]/", "", $default['de\_admin\_company\_tel']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo get\_text($mb['mb\_name']); ?></strong>님의 회원가입을 진심으로 축하합니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $mb['mb\_id'] ?></strong><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\register\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $mb['mb\_email'] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['opener\_href\_wr\_id'] ?>" class="scrap\_tit" target="\_blank" onclick="opener.document.location.href='<?php echo $list[$i]['opener\_href\_wr\_id'] ?>'; return false;"><?php echo $list[$i]['subject'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['opener\_href'] ?>" class="scrap\_cate" target="\_blank" onclick="opener.document.location.href='<?php echo $list[$i]['opener\_href'] ?>'; return false;"><?php echo $list[$i]['bo\_subject'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="scrap\_datetime"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$i]['ms\_datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['del\_href']; ?>" onclick="del(this.href); return false;" class="scrap\_del"><i class="fa fa-trash-o" aria-hidden="true"></i><span class="sound\_only">삭제</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($i == 0) echo "<li class=\"empty\_li\">자료가 없습니다.</li>"; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($config['cf\_write\_pages'], $page, $total\_page, "?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\scrap\_popin.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\scrap\_popin.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\member\basic\scrap\_popin.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_text(cut\_str($write['wr\_subject'], 255)) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $group\_select ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_id" value="<?php echo $mb\_id ?>" id="mb\_id" required class="frm\_input" size="40">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.getElementById("gr\_id").value = "<?php echo $gr\_id ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.getElementById("view").value = "<?php echo $view ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="view" value="<?php echo $view; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_bn\_id[]" value="<?php echo $i; ?>" id="chk\_bn\_id\_<?php echo $i; ?>" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_bn\_id\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<b class="sound\_only"><?php echo $num?>번</b>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table[<?php echo $i; ?>]" value="<?php echo $list[$i]['bo\_table']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id[<?php echo $i; ?>]" value="<?php echo $list[$i]['wr\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_group"><a href="./new.php?gr\_id=<?php echo $list[$i]['gr\_id'] ?>"><?php echo $gr\_subject ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_board"><a href="<?php echo get\_pretty\_url($list[$i]['bo\_table']); ?>"><?php echo $bo\_subject ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><a href="<?php echo $list[$i]['href'] ?>" class="new\_tit"><?php echo $list[$i]['comment'] ?><?php echo $wr\_subject ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_name"><?php echo $list[$i]['name'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_date"><?php echo $list[$i]['datetime2'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">게시물이 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\basic\outlogin.skin.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="foutlogin" action="<?php echo $outlogin\_action\_url ?>" onsubmit="return fhead\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\basic\outlogin.skin.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="url" value="<?php echo $outlogin\_url ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($member['mb\_id']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $nick ?>님</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == 'super' || $is\_auth) { ?><a href="<?php echo correct\_goto\_url(G5\_ADMIN\_URL); ?>" class="btn\_admin btn" title="관리자"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $point; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $memo\_not\_read; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="scrap"><?php echo $mb\_scrap\_cnt; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\shop\_basic\outlogin.skin.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="foutlogin" action="<?php echo $outlogin\_action\_url ?>" onsubmit="return fhead\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\shop\_basic\outlogin.skin.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="url" value="<?php echo $outlogin\_url ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="profile\_img"><?php echo get\_member\_profile\_img($member['mb\_id'], 30, 30); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="profile\_name"><?php echo $nick ?></span>님

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo G5\_BBS\_URL ?>/point.php" target="\_blank" class="win\_point">포인트<strong><?php echo $point ?></strong></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo G5\_SHOP\_URL ?>/coupon.php" target="\_blank" class="win\_coupon">쿠폰<strong><?php echo number\_format(get\_shop\_member\_coupon\_count($member['mb\_id'], true)); ?></strong></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo G5\_BBS\_URL ?>/memo.php" target="\_blank" class="win\_memo"><span class="sound\_only">안 읽은</span>쪽지<strong><?php echo $memo\_not\_read ?></strong></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\shop\_side\outlogin.skin.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="foutlogin" action="<?php echo $outlogin\_action\_url ?>" onsubmit="return fhead\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\shop\_side\outlogin.skin.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="url" value="<?php echo $outlogin\_url ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\shop\_side\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($member['mb\_id']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\shop\_side\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == 'super' || $is\_auth) { ?><a href="<?php echo correct\_goto\_url(G5\_ADMIN\_URL); ?>" class="btn\_admin"><i class="fa fa-cog fa-fw"></i><span class="sound\_only">관리자</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\shop\_side\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $nick ?>님</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\shop\_side\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $point ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\shop\_side\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($cp\_count); ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\outlogin\shop\_side\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $memo\_not\_read ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="po\_id" value="<?php echo $po\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == "super") { ?><a href="<?php echo G5\_ADMIN\_URL ?>/poll\_form.php?w=u&amp;po\_id=<?php echo $po\_id ?>" class="btn\_admin" title="설문관리"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">설문관리</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo $po['po\_subject'] ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="gb\_poll" value="<?php echo $i ?>" id="gb\_poll\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="gb\_poll\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $po['po\_poll'.$i] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo " alert('권한 {$po['po\_level']} 이상의 회원만 투표에 참여하실 수 있습니다.'); return false; ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo " alert('권한 {$po['po\_level']} 이상의 회원만 결과를 보실 수 있습니다.'); return false; ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_all">전체 <?php echo $nf\_total\_po\_cnt ?>표</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $po\_subject ?> 결과</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php echo $poll\_1st\_class; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $list[$i]['content'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span style="width:<?php echo number\_format($list[$i]['rate'], 1) ?>%"></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="poll\_cnt"><?php echo $list[$i]['cnt'] ?> 표</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_percent"><?php echo number\_format($list[$i]['rate'], 1) ?> %</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $list2[$i]['pc\_name'] ?><span class="sound\_only">님의 의견</span></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list2[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_datetime"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list2[$i]['datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_cmt\_del"><?php if ($list2[$i]['del']) { echo $list2[$i]['del']."<i class=\"fa fa-trash-o\" aria-hidden=\"true\"></i><span class=\"sound\_only\">삭제</span></a>"; } ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list2[$i]['idea'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="po\_id" value="<?php echo $po\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_member) { ?><input type="hidden" name="pc\_name" value="<?php echo get\_text(cut\_str($member['mb\_nick'],255)) ?>"><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h3><span>기타의견</span><?php echo $po\_etc ?></h3>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_guest) { echo chk\_captcha\_js(); } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="po\_id" value="<?php echo $po\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == "super") { ?><a href="<?php echo G5\_ADMIN\_URL ?>/poll\_form.php?w=u&amp;po\_id=<?php echo $po\_id ?>" class="btn\_admin"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">설문관리</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo $po['po\_subject'] ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="gb\_poll" value="<?php echo $i ?>" id="gb\_poll\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="gb\_poll\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $po['po\_poll'.$i] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo " alert('권한 {$po['po\_level']} 이상의 회원만 투표에 참여하실 수 있습니다.'); return false; ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo " alert('권한 {$po['po\_level']} 이상의 회원만 결과를 보실 수 있습니다.'); return false; ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_all">전체 <?php echo $nf\_total\_po\_cnt ?>표</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $po\_subject ?> 결과</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $list[$i]['content'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span style="width:<?php echo number\_format($list[$i]['rate'], 1) ?>%"></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="poll\_cnt"><?php echo $list[$i]['cnt'] ?> 표</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_percent"><?php echo number\_format($list[$i]['rate'], 1) ?> %</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $list2[$i]['pc\_name'] ?><span class="sound\_only">님의 의견</span></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list2[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_datetime"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list2[$i]['datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_cmt\_del"><?php if ($list2[$i]['del']) { echo $list2[$i]['del']."<i class=\"fa fa-trash-o\" aria-hidden=\"true\"></i><span class=\"sound\_only\">삭제</span></a>"; } ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list2[$i]['idea'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="po\_id" value="<?php echo $po\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_member) { ?><input type="hidden" name="pc\_name" value="<?php echo get\_text(cut\_str($member['mb\_nick'],255)) ?>"><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h3><span>기타의견</span><?php echo $po\_etc ?></h3>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_guest) { echo chk\_captcha\_js(); } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $qaconfig['qa\_title'] ?> 카테고리</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>Total <?php echo number\_format($total\_count) ?>건</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $page ?> 페이지

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($admin\_href) { ?><li><a href="<?php echo $admin\_href ?>" class="btn\_admin btn" title="관리자"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_qa\_sfl\_select\_options($sfl); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo stripslashes($stx); ?>" id="stx" required class="sch\_input" size="25" maxlength="15" placeholder=" 검색어를 입력해주세요">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b01 btn" title="문의등록"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">문의등록</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo get\_text($token); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $board['bo\_subject'] ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $lt\_class ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_qa\_id[]" value="<?php echo $list[$i]['qa\_id'] ?>" id="chk\_qa\_id\_<?php echo $i ?>" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_qa\_id\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<b class="sound\_only"><?php echo $list[$i]['subject'] ?></b>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $list[$i]['num']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_cate\_link"><?php echo $list[$i]['category']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['view\_href']; ?>" class="bo\_tit">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['subject']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['icon\_file']) echo " <i class=\"fa fa-download\" aria-hidden=\"true\"></i>" ; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_name"><?php echo $list[$i]['name']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_date"><?php echo $list[$i]['date']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_stat"><span class=" <?php echo ($list[$i]['qa\_status'] ? 'txt\_done' : 'txt\_rdy'); ?>"><?php echo ($list[$i]['qa\_status'] ? '답변완료' : '답변대기'); ?></span></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($i == 0) { echo '<tr><td colspan="'.$colspan.'" class="empty\_table">게시물이 없습니다.</td></tr>'; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list\_pages; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list\_href) { ?><li><a href="<?php echo $list\_href ?>" class="btn\_b01 btn" title="목록"><i class="fa fa-list" aria-hidden="true"></i><span class="sound\_only">목록</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b01 btn" title="문의등록"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">문의등록</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><span class="bo\_v\_reply">답변</span> <?php echo get\_text($answer['qa\_subject']); ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $answer['qa\_datetime']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $answer\_update\_href; ?>" class="btn\_b01 btn" title="답변수정">답변수정</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $answer\_delete\_href; ?>" class="btn\_b01 btn" onclick="del(this.href); return false;" title="답변삭제">답변삭제</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_view\_thumbnail(conv\_content($answer['qa\_content'], $answer['qa\_html']), $qaconfig['qa\_image\_width']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $rewrite\_href; ?>" class="add\_qa" title="추가질문">추가질문</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qa\_id" value="<?php echo $view['qa\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo $token ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_hidden;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $option; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="qa\_content\_wrap <?php echo $is\_dhtml\_editor ? $config['cf\_editor'] : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<span class="bo\_v\_cate">'.$view['category'].'</span> ';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $view['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자</span><strong><?php echo $view['name'] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성일</span><strong class="bo\_date"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $view['datetime']; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><i class="fa fa-envelope-o" aria-hidden="true"></i> <?php echo $view['email']; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><i class="fa fa-phone" aria-hidden="true"></i> <?php echo $view['hp']; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $list\_href ?>" class="btn\_b01 btn" title="목록"><i class="fa fa-list" aria-hidden="true"></i><span class="sound\_only">목록</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b01 btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($update\_href) { ?><li><a href="<?php echo $update\_href ?>" class="btn\_b01 btn" title="수정">수정<i class="fa fa-pencil-square-o" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($delete\_href) { ?><li><a href="<?php echo $delete\_href ?>" class="btn\_b01 btn" onclick="del(this.href); return false;" title="삭제">삭제<i class="fa fa-trash-o" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_view\_thumbnail($view['img\_file'][$i], $qaconfig['qa\_image\_width']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="bo\_v\_con"><?php echo get\_view\_thumbnail($view['content'], $qaconfig['qa\_image\_width']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="bo\_v\_addq"><a href="<?php echo $rewrite\_href; ?>" class="btn\_b01">추가질문</a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['download\_href'][$i]; ?>" class="view\_file\_download" download>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $view['download\_source'][$i] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($prev\_href) { ?><li><a href="<?php echo $prev\_href ?>" class="btn\_b01 btn"><i class="fa fa-chevron-left" aria-hidden="true"></i> 이전글</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($next\_href) { ?><li><a href="<?php echo $next\_href ?>" class="btn\_b01 btn">다음글 <i class="fa fa-chevron-right" aria-hidden="true"></i></a></li><?php } ?>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($qa\_skin\_path.'/view.answer.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($qa\_skin\_path.'/view.answerform.skin.php');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_cate\_link"><?php echo get\_text($rel\_list[$i]['category']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $rel\_list[$i]['view\_href']; ?>" class="bo\_tit">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $rel\_list[$i]['subject']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_date"><?php echo $rel\_list[$i]['date']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_stat"><span class="<?php echo ($rel\_list[$i]['qa\_status'] ? 'txt\_done' : 'txt\_rdy'); ?>"><?php echo ($rel\_list[$i]['qa\_status'] ? '<i class="fa fa-check-circle" aria-hidden="true"></i> 답변완료' : '<i class="fa fa-times-circle" aria-hidden="true"></i> 답변대기'); ?></span></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fwrite" id="fwrite" action="<?php echo $action\_url ?>" onsubmit="return fwrite\_submit(this);" method="post" enctype="multipart/form-data" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qa\_id" value="<?php echo $qa\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo $token ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_hidden;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_email" value="<?php echo get\_text($write['qa\_email']); ?>" id="qa\_email" <?php echo $req\_email; ?> class="<?php echo $req\_email.' '; ?>frm\_input full\_input email" size="50" maxlength="100" placeholder="이메일">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qa\_email\_recv" id="qa\_email\_recv" value="1" <?php if($write['qa\_email\_recv']) echo 'checked="checked"'; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_hp" value="<?php echo get\_text($write['qa\_hp']); ?>" id="qa\_hp" <?php echo $req\_hp; ?> class="<?php echo $req\_hp.' '; ?>frm\_input full\_input" size="30" placeholder="휴대폰">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qa\_sms\_recv" id="qa\_sms\_recv" value="1" <?php if($write['qa\_sms\_recv']) echo 'checked="checked"'; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_subject" value="<?php echo get\_text($write['qa\_subject']); ?>" id="qa\_subject" required class="frm\_input full\_input required" size="50" maxlength="255" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="qa\_content\_wrap <?php echo $is\_dhtml\_editor ? $config['cf\_editor'] : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $option; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="file" name="bf\_file[1]" id="bf\_file\_1" title="파일첨부 1 : 용량 <?php echo $upload\_max\_filesize; ?> 이하만 업로드 가능" class="frm\_file">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="bf\_file\_del1" name="bf\_file\_del[1]" value="1"> <label for="bf\_file\_del1"><?php echo $write['qa\_source1']; ?> 파일 삭제</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="file" name="bf\_file[2]" id="bf\_file\_2" title="파일첨부 2 : 용량 <?php echo $upload\_max\_filesize; ?> 이하만 업로드 가능" class="frm\_file">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="bf\_file\_del2" name="bf\_file\_del[2]" value="1"> <label for="bf\_file\_del2"><?php echo $write['qa\_source2']; ?> 파일 삭제</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list\_href; ?>" class="btn\_cancel btn">취소</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="srows" value="<?php echo $srows ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $group\_select ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<script>document.getElementById("gr\_id").value = "<?php echo $gr\_id ?>";</script>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="wr\_subject||wr\_content"<?php echo get\_selected($sfl, "wr\_subject||wr\_content") ?>>제목+내용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="wr\_subject"<?php echo get\_selected($sfl, "wr\_subject") ?>>제목</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="wr\_content"<?php echo get\_selected($sfl, "wr\_content") ?>>내용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mb\_id"<?php echo get\_selected($sfl, "mb\_id") ?>>회원아이디</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="wr\_name"<?php echo get\_selected($sfl, "wr\_name") ?>>이름</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $text\_stx ?>" id="stx" required class="frm\_input" size="40">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" value="and" <?php echo ($sop == "and") ? "checked" : ""; ?> id="sop\_and" name="sop">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" value="or" <?php echo ($sop == "or") ? "checked" : ""; ?> id="sop\_or" name="sop" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><strong><?php echo $stx ?></strong> 전체검색 결과</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li>게시판 <?php echo $board\_count ?>개</li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li>게시물 <?php echo number\_format($total\_count) ?>개</li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><?php echo number\_format($page) ?>/<?php echo number\_format($total\_page) ?> 페이지 열람 중</li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="?<?php echo $search\_query ?>&amp;gr\_id=<?php echo $gr\_id ?>" <?php echo $sch\_all ?>>전체게시판</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str\_board\_list; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><a href="<?php echo get\_pretty\_url($search\_table[$idx], '', $search\_query); ?>"><?php echo $bo\_subject[$idx] ?> 게시판 내 결과</a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($search\_table[$idx], '', $search\_query); ?>" class="sch\_more">더보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$idx][$i]['href'] ?><?php echo $comment\_href ?>" class="sch\_res\_title"><?php echo $comment\_def ?><?php echo $list[$idx][$i]['subject'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$idx][$i]['href'] ?><?php echo $comment\_href ?>" target="\_blank" class="pop\_a"><i class="fa fa-window-restore" aria-hidden="true"></i><span class="sound\_only">새창</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo $list[$idx][$i]['content'] ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$idx][$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sch\_datetime"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$idx][$i]['wr\_datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxbanner.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i==0) echo '<aside id="sbn\_side" class="sbn"><h2>쇼핑몰 배너</h2><ul class="sb\_bn">'.PHP\_EOL;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxbanner.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

echo $banner.'<img src="'.G5\_DATA\_URL.'/banner/'.$row['bn\_id'].'?'.preg\_replace('/[^0-9]/i', '', $row['bn\_time']).'" alt="'.get\_text($row['bn\_alt']).'" width="'.$size[0].'" height="'.$size[1].'"'.$bn\_border.'>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxbanner.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $banner.'<img src="'.G5\_DATA\_URL.'/banner/'.$row['bn\_id'].'?'.preg\_replace('/[^0-9]/i', '', $row['bn\_time']).'" alt="'.get\_text($row['bn\_alt']).'" width="'.$size[0].'" height="'.$size[1].'"'.$bn\_border.'>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxbanner.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i>0) echo '</ul></aside>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxcart.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="prd\_img">'.$it\_img.'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxcart.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="'.G5\_SHOP\_URL.'/cart.php" class="prd\_name">'.$it\_name.'</a>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxcart.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo number\_format($row['ct\_price']).PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxcart.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<button class="cart\_del" type="button" data-it\_id="'.$row['it\_id'].'"><i class="fa fa-trash-o" aria-hidden="true"></i><span class="sound\_only">삭제</span></button>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxcart.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="hidden" name="ct\_chk['.$i.']" value="1">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxcart.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="hidden" name="it\_id['.$i.']" value="'.$row['it\_id'].'">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxcart.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="hidden" name="it\_name['.$i.']" value="'.$it\_name.'">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxcategory.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="gnb\_1dli" style="z-index:<?php echo $gnb\_zindex; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxcategory.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $row['url']; ?>" class="gnb\_1da"><?php echo $row['ca\_name']; ?><?php if ($count) echo '<i class="fa fa-angle-right" aria-hidden="true"></i>'; ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxcategory.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($j==0) echo '<ul class="gnb\_2dul" style="z-index:'.$gnb\_zindex.'">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxcategory.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="gnb\_2dli"><a href="<?php echo $row2['url']; ?>" class="gnb\_2da"><?php echo $row2['ca\_name']; ?></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxcategory.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($j>0) echo '</ul>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxcommunity.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><i class="fa fa-angle-right" aria-hidden="true"></i> <a href="'.get\_pretty\_url($row['bo\_table']).'">'.$row['bo\_subject'].'</a></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="'.$href.'" class="sev\_img"><img src="'.G5\_DATA\_URL.'/event/'.$row['ev\_id'].'\_m" alt="'.$row['ev\_subject'].'"></a>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="'.$href.'" class="sev\_text">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($row['ev\_subject\_strong']) echo '<strong>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $row['ev\_subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($row['ev\_subject\_strong']) echo '</strong>';

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxevent.skin.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

from `{$g5['g5\_shop\_event\_item\_table']}` a left join `{$g5['g5\_shop\_item\_table']}` b on (a.it\_id = b.it\_id)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li class="ev\_prd\_'.$k.'">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<span class="ev\_prd\_img">'.get\_it\_image($row2['it\_id'], 110, 110, get\_text($row2['it\_name'])).'</span>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="ev\_txt\_wr"><a href="'.$item\_href.'" class="ev\_prd\_tit">'.get\_text(cut\_str($row2['it\_name'], 30)).'</a>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<span class="ev\_prd\_price">'.display\_price(get\_price($row2), $row2['it\_tel\_inq']).'</span></div>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><a href="'.$href.'" class="sev\_more">더보기</a></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($tv\_tot\_count == 0) echo '<ul id="stv\_ul">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li class="stv\_item c'.$k.'">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $img;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo cut\_str($it\_name, 10, '').PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $print\_price.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($tv\_tot\_count > 0) echo '</ul>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var itemQty = <?php echo $tv\_tot\_count; ?>;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var itemShow = <?php echo $tv\_div['img\_length']; ?>;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var EOFlag = parseInt(<?php echo $i-1; ?>/itemShow);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var itemRest = parseInt(<?php echo $i-1; ?>%itemShow);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxwish.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="prd\_img">'.$it\_img.'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxwish.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="'.shop\_item\_url($row['it\_id']).'" class="prd\_name">'.$it\_name.'</a>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\boxwish.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="prd\_price">'.display\_price(get\_price($item), $item['it\_tel\_inq']).'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\couponzone.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo $default['de\_admin\_company\_name']; ?> 회원이시라면 쿠폰 다운로드 후 바로 사용하실 수 있습니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\couponzone.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<ul>'.PHP\_EOL.$coupon.'</ul>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\couponzone.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p>보유하신 <?php echo $default['de\_admin\_company\_name']; ?> 회원 포인트를 쿠폰으로 교환하실 수 있습니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\couponzone.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<ul>'.PHP\_EOL.$coupon.'</ul>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fitem" method="post" action="<?php echo $action\_url; ?>" onsubmit="return fitem\_submit(this);">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[]" value="<?php echo $it\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="'.G5\_SHOP\_URL.'/largeimage.php?it\_id='.$it['it\_id'].'&amp;no='.$i.'" target="\_blank" class="popup\_item\_image">'.$img.'</a>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_SHOP\_URL; ?>/largeimage.php?it\_id=<?php echo $it['it\_id']; ?>&amp;no=1" target="\_blank" id="popup\_item\_image" class="popup\_item\_image"><i class="fa fa-search-plus" aria-hidden="true"></i><span class="sound\_only">확대보기</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li '.$sit\_pvi\_last.'>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="'.G5\_SHOP\_URL.'/largeimage.php?it\_id='.$it['it\_id'].'&amp;no='.$thumb\_count.'" target="\_blank" class="popup\_item\_image img\_thumb">'.$val.'<span class="sound\_only"> '.$thumb\_count.'번째 이미지 새창</span></a>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 id="sit\_title"><?php echo stripslashes($it['it\_name']); ?> <span class="sound\_only">요약정보 및 구매</span></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p id="sit\_desc"><?php echo $it['it\_basic']; ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

상품 선택옵션 <?php echo $option\_count; ?> 개, 추가옵션 <?php echo $supply\_count; ?> 개

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<img src="<?php echo G5\_SHOP\_URL; ?>/img/s\_star<?php echo $star\_score?>.png" alt="" class="sit\_star" width="100">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">별<?php echo $star\_score?>개</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="">사용후기 <?php echo $it['it\_use\_cnt']; ?> 개</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="btn\_wish"><i class="fa fa-heart-o" aria-hidden="true"></i><span class="sound\_only">위시리스트</span><span class="btn\_wish\_num"><?php echo get\_wishlist\_count\_by\_item($it['it\_id']); ?></span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $sns\_share\_links; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:popup\_item\_recommend('<?php echo $it['it\_id']; ?>');" id="sit\_btn\_rec"><i class="fa fa-envelope-o" aria-hidden="true"></i><span class="sound\_only">추천하기</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_price($it['it\_cust\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo display\_price(get\_price($it)); ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="it\_price" value="<?php echo get\_price($it); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $it['it\_maker']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $it['it\_origin']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $it['it\_brand']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $it['it\_model']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '구매금액(추가옵션 제외)의 '.$it['it\_point'].'%';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 183 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo number\_format($it\_point).'점';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 209 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th><?php echo $ct\_send\_cost\_label; ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 210 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $sc\_method; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 215 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($it['it\_buy\_min\_qty']); ?> 개</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 221 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($it['it\_buy\_max\_qty']); ?> 개</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 235 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_item;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 250 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $supply\_item;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 269 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_type[<?php echo $it\_id; ?>][]" value="0">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 270 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_id[<?php echo $it\_id; ?>][]" value="">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 271 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_value[<?php echo $it\_id; ?>][]" value="<?php echo $it['it\_name']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 273 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" class="io\_stock" value="<?php echo $it['it\_stock\_qty']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 275 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sit\_opt\_subj"><?php echo $it['it\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 278 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ct\_qty\_<?php echo $i; ?>" class="sound\_only">수량</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 280 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ct\_qty[<?php echo $it\_id; ?>][]" value="<?php echo $it['it\_buy\_min\_qty']; ?>" id="ct\_qty\_<?php echo $i; ?>" class="num\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 308 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:item\_wish(document.fitem, '<?php echo $it['it\_id']; ?>');" class="sit\_btn\_wish"><i class="fa fa-heart-o" aria-hidden="true"></i><span class="sound\_only">위시리스트</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 311 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:popup\_stocksms('<?php echo $it['it\_id']; ?>');" id="sit\_btn\_alm">재입고알림</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 314 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="itemform-naverpay"><?php echo $naverpay\_request\_js.$naverpay\_button\_js; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 358 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $prev\_href.$prev\_title.$prev\_href2;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 359 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $next\_href.$next\_title.$next\_href2;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 408 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var min\_qty = parseInt(<?php echo $it['it\_buy\_min\_qty']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 409 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var max\_qty = parseInt(<?php echo $it['it\_buy\_max\_qty']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 458 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

f.action = "<?php echo $action\_url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 480 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var min\_qty = parseInt(<?php echo $it['it\_buy\_min\_qty']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 481 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var max\_qty = parseInt(<?php echo $it['it\_buy\_max\_qty']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><button type="button" id="btn\_sit\_use" rel="#sit\_use">사용후기 <span class="item\_use\_count"><?php echo $item\_use\_count; ?></span></button></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><button type="button" id="btn\_sit\_qa" rel="#sit\_qa">상품문의 <span class="item\_qa\_count"><?php echo $item\_qa\_count; ?></span></button></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($it['it\_explan'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><?php echo $ii\_title; ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $ii\_value; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($default['de\_baesong\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($default['de\_change\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo str\_replace(array('class="get\_item\_options"', 'id="it\_option\_', 'class="it\_option"'), array('class="get\_side\_item\_options"', 'id="it\_side\_option\_', 'class="it\_side\_option"'), $option\_item);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo str\_replace(array('id="it\_supply\_', 'class="it\_supply"'), array('id="it\_side\_supply\_', 'class="it\_side\_supply"'), $supply\_item);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sit\_opt\_subj"><?php echo $it['it\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 169 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ct\_qty\_<?php echo $i; ?>" class="sound\_only">수량</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ct\_copy\_qty[<?php echo $it\_id; ?>][]" value="<?php echo $it['it\_buy\_min\_qty']; ?>" id="ct\_qty\_<?php echo $i; ?>" class="num\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemqa\_form; ?>" class="btn02 itemqa\_form">상품문의 쓰기<span class="sound\_only">새 창</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemqa\_list; ?>" id="itemqa\_list" class="btn01">더보기</a>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqa.skin.php

MD5 Hashing algorithm.

$hash = md5($row['iq\_id'].$row['iq\_time'].$row['iq\_ip']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<ol id="sit\_qa\_ol">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" class="sit\_qa\_li\_title"><span class="<?php echo $iq\_style; ?>"><?php echo $iq\_stats; ?></span><?php echo $iq\_subject; ?></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo $iq\_name; ?><span class="st\_bg"></span><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $iq\_time; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sit\_qa\_con\_<?php echo $i; ?>" class="sit\_qa\_con">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $iq\_question;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $iq\_answer; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemqa\_form."&amp;iq\_id={$row['iq\_id']}&amp;w=u"; ?>" class="itemqa\_form btn01" onclick="return false;">수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemqa\_formupdate."&amp;iq\_id={$row['iq\_id']}&amp;w=d&amp;hash={$hash}"; ?>" class="itemqa\_delete btn01">삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo '</ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (!$i) echo '<p class="sit\_empty">상품문의가 없습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo itemqa\_page($config['cf\_write\_pages'], $page, $total\_page, G5\_SHOP\_URL."/itemqa.php?it\_id=$it\_id&amp;page=", "");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id" value="<?php echo $it\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="iq\_id" value="<?php echo $iq\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="iq\_secret" id="iq\_secret" value="1" <?php echo $chk\_secret; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="iq\_email" id="iq\_email" value="<?php echo get\_text($qa['iq\_email']); ?>" class="frm\_input full\_input" size="30" placeholder="이메일"><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="iq\_hp" id="iq\_hp" value="<?php echo get\_text($qa['iq\_hp']); ?>" class="frm\_input full\_input" size="20" placeholder="휴대폰"><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="iq\_subject" value="<?php echo get\_text($qa['iq\_subject']); ?>" id="iq\_subject" required class="required frm\_input" maxlength="250" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form method="get" action="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="b.it\_name" <?php echo get\_selected($sfl, "b.it\_name", true); ?>>상품명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.it\_id" <?php echo get\_selected($sfl, "a.it\_id"); ?>>상품코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.iq\_subject" <?php echo get\_selected($sfl, "a.iq\_subject"); ?>>문의제목</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.iq\_question"<?php echo get\_selected($sfl, "a.iq\_question"); ?>>문의내용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.iq\_name" <?php echo get\_selected($sfl, "a.iq\_name"); ?>>작성자명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.mb\_id" <?php echo get\_selected($sfl, "a.mb\_id"); ?>>작성자아이디</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx; ?>" id="stx" required class="sch\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">전체보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <p><?php echo $config['cf\_title']; ?> 전체 상품문의 목록입니다.</p> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $it\_href; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_it\_image($row['it\_id'], 50, 50); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $row['it\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $iq\_subject; ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="<?php echo $iq\_style; ?>"><?php echo $iq\_stats; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><i class="fa fa-user" aria-hidden="true"></i> <?php echo $row['iq\_name']; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo substr($row['iq\_time'],0,10); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sqa\_con\_<?php echo $i; ?>" class="sqa\_con" style="display:none;">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $iq\_question;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $iq\_answer; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sqa\_con\_btn"><button class="sqa\_con\_<?php echo $i; ?>">내용보기 <i class="fa fa-caret-down" aria-hidden="true"></i></button></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo '</ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<p id="sqa\_empty">자료가 없습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h4>구매고객 총평점 <span>(총 <strong><?php echo $total\_count; ?></strong> 건 상품평 기준)</span></h4>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<img src="<?php echo G5\_SHOP\_URL; ?>/img/s\_star<?php echo $star\_score?>.png" alt="" class="sit\_star">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemuse\_form; ?>" class="btn02 itemuse\_form">사용후기 쓰기<span class="sound\_only"> 새 창</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemuse\_list; ?>" class="btn01 itemuse\_list">더보기</a>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

MD5 Hashing algorithm.

$hash = md5($row['is\_id'].$row['is\_time'].$row['is\_ip']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<ol id="sit\_use\_ol">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sit\_thum"><?php echo get\_itemuselist\_thumbnail($row['it\_id'], $row['is\_content'], 100, 100); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sit\_use\_star"><img src="<?php echo G5\_SHOP\_URL; ?>/img/s\_star<?php echo $is\_star; ?>.png" alt="별<?php echo $is\_star; ?>개" width="85"></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sit\_use\_tit"><?php echo $is\_subject; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo $is\_name; ?><span class="st\_bg"></span><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $is\_time; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sit\_use\_con\_<?php echo $i; ?>" class="sit\_use\_con">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemuse\_form."&amp;is\_id={$row['is\_id']}&amp;w=u"; ?>" class="itemuse\_form btn01" onclick="return false;">수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemuse\_formupdate."&amp;is\_id={$row['is\_id']}&amp;w=d&amp;hash={$hash}"; ?>" class="itemuse\_delete btn01">삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_reply\_subject;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_reply\_name;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_reply\_content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo '</ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (!$i) echo '<p class="sit\_empty">사용후기가 없습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo itemuse\_page($config['cf\_write\_pages'], $page, $total\_page, G5\_SHOP\_URL."/itemuse.php?it\_id=$it\_id&amp;page=", "");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id" value="<?php echo $it\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="is\_id" value="<?php echo $is\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="is\_subject" value="<?php echo get\_text($use['is\_subject']); ?>" id="is\_subject" required class="required frm\_input full\_input" maxlength="250" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="5" id="is\_score5" <?php echo ($is\_score==5)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="4" id="is\_score4" <?php echo ($is\_score==4)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="3" id="is\_score3" <?php echo ($is\_score==3)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="2" id="is\_score2" <?php echo ($is\_score==2)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="1" id="is\_score1" <?php echo ($is\_score==1)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form method="get" action="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="b.it\_name" <?php echo get\_selected($sfl, "b.it\_name"); ?>>상품명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.it\_id" <?php echo get\_selected($sfl, "a.it\_id"); ?>>상품코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.is\_subject"<?php echo get\_selected($sfl, "a.is\_subject"); ?>>후기제목</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.is\_content"<?php echo get\_selected($sfl, "a.is\_content"); ?>>후기내용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.is\_name" <?php echo get\_selected($sfl, "a.is\_name"); ?>>작성자명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.mb\_id" <?php echo get\_selected($sfl, "a.mb\_id"); ?>>작성자아이디</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx; ?>" id="stx" required class="sch\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">전체보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <p><?php echo $config['cf\_title']; ?> 전체 사용후기 목록입니다.</p> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $it\_href; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_it\_image($row['it\_id'], 100, 100); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $row2['it\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button class="prd\_detail" data-url="<?php echo G5\_SHOP\_URL.'/largeimage.php?it\_id='.$row['it\_id']; ?>"><i class="fa fa-camera" aria-hidden="true"></i><span class="sound\_only">상품 이미지보기</span></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><img src="<?php echo G5\_URL; ?>/shop/img/s\_star<?php echo $star; ?>.png" alt="별<?php echo $star; ?>개" width="80"></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sps\_pd\_name"><?php echo get\_text($row2['it\_name']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sps\_rv\_tit"><?php echo get\_text($row['is\_subject']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sps\_rv\_thum"><?php echo get\_itemuse\_thumb($row['is\_content'], 60, 60); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><i class="fa fa-user" aria-hidden="true"></i> <?php echo $row['is\_name']; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo substr($row['is\_time'],0,10); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button class="sps\_con\_<?php echo $i; ?> review\_detail">내용보기</button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo get\_text($row['is\_subject']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><i class="fa fa-user" aria-hidden="true"></i> <?php echo $row['is\_name']; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo substr($row['is\_time'],0,10); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_it\_image($row['it\_id'], 50, 50); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo get\_text($row2['it\_name']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">평가점수</span><img src="<?php echo G5\_URL; ?>/shop/img/s\_star<?php echo $star; ?>.png" alt="별<?php echo $star; ?>개" width="80">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sps\_con\_<?php echo $i; ?>" class="review\_bt\_cnt">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="is\_use\_reply"><?php echo get\_text($row['is\_reply\_subject']); ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $row['is\_reply\_name']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sps\_con\_<?php echo $i; ?>\_reply">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_reply\_content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo '</ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<p id="sps\_empty">자료가 없습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\largeimage.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $imgs['imagehtml']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\largeimage.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><a href="'.G5\_SHOP\_URL.'/largeimage.php?it\_id='.$it\_id.'&amp;no='.$key.'" class="img\_thumb">'.$val.'</a></li>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\largeimage.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$("#sit\_pvi\_nwbig span:eq("+<?php echo ($no - 1); ?>+")").addClass("visible");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\largeimage.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

largeimage\_load(<?php echo $size[0]; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li ".implode(' ', $classes)."\" data-css=\"nocss\" style=\"height:auto\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_star\"><span class=\"sound\_only\">고객평점</span><img src=\"".G5\_SHOP\_URL."/img/s\_star".$star\_score.".png\" alt=\"별점 ".$star\_score."점\" class=\"sit\_star\"></div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_basic\">".stripslashes($row['it\_basic'])."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<span class=\"sct\_dict\">".display\_price($row['it\_cust\_price'])."</span>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<button type=\"button\" class=\"btn\_wish\" data-it\_id=\"{$row['it\_id']}\"><span class=\"sound\_only\">위시리스트</span><i class=\"fa fa-heart-o\" aria-hidden=\"true\"></i></button>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/facebook.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/twitter.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/gplus.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sit\_icon\_li\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i >= 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i === 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$sct\_last}\" data-css=\"nocss\" style=\"width:{$this->img\_width}px\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_icon\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_basic\">".stripslashes($row['it\_basic'])."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<span class=\"sct\_dict\">".display\_price($row['it\_cust\_price'])."</span>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/sns\_fb\_s.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/sns\_twt\_s.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/sns\_goo\_s.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i >= 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$sct\_last}\" data-css=\"nocss\" style=\"padding:{$list\_top\_pad}px {$list\_right\_pad}px {$list\_bottom\_pad}px {$list\_left\_pad}px;width:{$list\_width}px;height:{$list\_height}px\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_icon\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_basic\">".stripslashes($row['it\_basic'])."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<span class=\"sct\_dict\">".display\_price($row['it\_cust\_price'])."</span>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/sns\_fb\_s.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/sns\_twt\_s.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/sns\_goo\_s.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_arw\_toleft\" style=\"left:{$arrow\_left}px\"></div>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i >= 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$sct\_last}\" data-css=\"nocss\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_icon\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_basic\">".stripslashes($row['it\_basic'])."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<span class=\"sct\_dict\">".display\_price($row['it\_cust\_price'])."</span>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<button type=\"button\" class=\"btn\_wish\" data-it\_id=\"{$row['it\_id']}\"><span class=\"sound\_only\">위시리스트</span><i class=\"fa fa-heart-o\" aria-hidden=\"true\"></i></button>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/facebook.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/twitter.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/gplus.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_rel\">".relation\_item($row['it\_id'], 70, 0, 5)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i >= 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_name&amp;sortodr=asc">상품명순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_type1&amp;sortodr=desc">히트상품</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_type2&amp;sortodr=desc">추천상품</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_type3&amp;sortodr=desc">최신상품</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_type4&amp;sortodr=desc">인기상품</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_type5&amp;sortodr=desc">할인상품</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_sum\_qty&amp;sortodr=desc">판매많은순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_price&amp;sortodr=asc">낮은가격순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_price&amp;sortodr=desc">높은가격순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_use\_avg&amp;sortodr=desc">평점높은순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_use\_cnt&amp;sortodr=desc">후기많은순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_update\_time&amp;sortodr=desc">최근등록순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\listcategory.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\listcategory2.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\listcategory3.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"sct smt\_40 owl-carousel\" data-value=\"".$this->list\_mod."\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li {$sct\_last}\" style=\"width:{$this->img\_width}px\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_star\"><span class=\"sound\_only\">고객평점</span><img src=\"".G5\_SHOP\_URL."/img/s\_star".$star\_score.".png\" alt=\"별점 ".$star\_score."점\" class=\"sit\_star\"></div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i >= 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<ul id="btn\_smt\_<?php echo $this->type; ?>" class="sctrl">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div id=\"smt\_{$this->type}\" class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div id=\"smt\_{$this->type}\" class=\"sct smt\_20\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$sct\_last}\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_basic\">".stripslashes($row['it\_basic'])."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<span class=\"sct\_dict\">".display\_price($row['it\_cust\_price'])."</span>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_sns\" style=\"top:{$sns\_top}px\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/facebook.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/twitter.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/gplus.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_icon\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 254 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$("#smt\_<?php echo $this->type; ?>").topRolling();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 259 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$("#btn\_smt\_<?php echo $this->type; ?> button.sctrl\_play").on("click", function() {

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 260 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$("#btn\_smt\_<?php echo $this->type; ?> button.sctrl\_stop").data("stop", false);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 268 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$("#btn\_smt\_<?php echo $this->type; ?> button.sctrl\_stop").on("click", function() {

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$sct\_last}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<span class="sct\_disc">'.$sale\_per.'</span>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_star\"><span class=\"sound\_only\">고객평점</span><img src=\"".G5\_SHOP\_URL."/img/s\_star".$star\_score.".png\" alt=\"별점 ".$star\_score."점\" class=\"sit\_star\"></div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_basic\">".stripslashes($row['it\_basic'])."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<span class=\"sct\_dict\">".display\_price($row['it\_cust\_price'])."</span>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<button type=\"button\" class=\"btn\_wish\" data-it\_id=\"{$row['it\_id']}\"><span class=\"sound\_only\">위시리스트</span><i class=\"fa fa-heart-o\" aria-hidden=\"true\"></i></button>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/facebook.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/twitter.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/gplus.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sit\_icon\_li\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i >= 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$sct\_last}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_star\"><span class=\"sound\_only\">고객평점</span><img src=\"".G5\_SHOP\_URL."/img/s\_star".$star\_score.".png\" alt=\"별점 ".$star\_score."점\" class=\"sit\_star\"></div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_basic\">".stripslashes($row['it\_basic'])."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<button type=\"button\" class=\"btn\_wish\" data-it\_id=\"{$row['it\_id']}\"><span class=\"sound\_only\">위시리스트</span><i class=\"fa fa-heart-o\" aria-hidden=\"true\"></i></button>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/facebook.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/twitter.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/gplus.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sit\_icon\_li\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i >= 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul id=\"smt\_{$this->type}\" class=\"smt\_30\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li sct\_li\_{$i}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<span class=\"sound\_only\">고객평점</span><img src=\"".G5\_SHOP\_URL."/img/s\_star".$star\_score.".png\" alt=\"별 ".$star\_score."개\" class=\"sit\_star\" width=\"100\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<span class=\"sct\_dict\">".display\_price($row['it\_cust\_price'])."</span>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i >= 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\mainbanner.10.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$item\_html .= $banner.'<img src="'.G5\_DATA\_URL.'/banner/'.$row['bn\_id'].'?'.preg\_replace('/[^0-9]/i', '', $row['bn\_time']).'" width="'.$size[0].'" alt="'.get\_text($row['bn\_alt']).'"'.$bn\_border.'>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\mainbanner.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i==0) echo '<div id="main\_bn" '.$banner\_style.'><div class="main\_banner\_owl owl-carousel">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\mainbanner.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $item\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\mainbanner.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li class="owl-dot"><a data-slide-index="'.$k.'" href="#">'.get\_text($row['bn\_alt']).'</a></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\navigation.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sct\_location" class="<?php echo implode(' ', $location\_class);?>"> <!-- class="view\_location" --> <!-- view\_location는 리스트 말고 상품보기에서만 표시 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\navigation.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $data['ca\_id']; ?>" data-url="<?php echo $data['url']; ?>" <?php if($ca\_ids['ca\_id'] === $data['ca\_id']) echo 'selected'; ?>><?php echo $data['ca\_name']; ?></option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\navigation.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $data['ca\_id']; ?>" data-url="<?php echo $data['url']; ?>" <?php if($ca\_ids['ca\_id2'] === $data['ca\_id']) echo 'selected'; ?>><?php echo $data['ca\_name']; ?></option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\navigation.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $data['ca\_id']; ?>" data-url="<?php echo $data['url']; ?>" <?php if($ca\_ids['ca\_id3'] === $data['ca\_id']) echo 'selected'; ?>><?php echo $data['ca\_name']; ?></option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\navigation.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_text($g5['title']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="sct\_li<?php echo $sct\_last; ?>" style="width:<?php echo $img\_width; ?>px">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sct\_img"><a href="<?php echo $href; ?>" class="sct\_a"><img src="<?php echo G5\_SHOP\_SKIN\_URL; ?>/img/personal.jpg" alt=""></a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sct\_txt"><a href="<?php echo $href; ?>" class="sct\_a"><?php echo get\_text($row['pp\_name']).'님 개인결제'; ?></a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sct\_cost"><?php echo display\_price($row['pp\_price']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 1) echo "<p class=\"sct\_noitem\">등록된 개인결제가 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li slide {$sct\_last}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_icon\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strike>".display\_price($row['it\_cust\_price'])."</strike>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_sns\" style=\"top:{$sns\_top}px\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/sns\_fb\_s.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/sns\_twt\_s.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/sns\_goo\_s.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 1) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><strong><?php echo $q; ?></strong> 검색 결과<span class="ssch\_result\_total">총 <?php echo $total\_count; ?>건</span></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qsort" id="qsort" value="<?php echo $qsort ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qorder" id="qorder" value="<?php echo $qorder ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qcaid" id="qcaid" value="<?php echo $qcaid ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="q" value="<?php echo $q; ?>" id="ssch\_q" class="ssch\_input" size="40" maxlength="30" placeholder="검색어">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qname" id="ssch\_qname" value="1" <?php echo $qname\_check?'checked="checked"':'';?>> <label for="ssch\_qname"><span></span>상품명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qexplan" id="ssch\_qexplan" value="1" <?php echo $qexplan\_check?'checked="checked"':'';?>> <label for="ssch\_qexplan"><span></span>상품설명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qbasic" id="ssch\_qbasic" value="1" <?php echo $qbasic\_check?'checked="checked"':'';?>> <label for="ssch\_qbasic"><span></span>기본설명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qid" id="ssch\_qid" value="1" <?php echo $qid\_check?'checked="checked"':'';?>> <label for="ssch\_qid"><span></span>상품코드</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qfrom" value="<?php echo $qfrom; ?>" id="ssch\_qfrom" class="ssch\_input" size="10"> 원 ~

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qto" value="<?php echo $qto; ?>" id="ssch\_qto" class="ssch\_input" size="10"> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><a href="#" onclick="set\_ca\_id(\'\'); return false;">전체분류 <span>('.$total\_count.')</span></a></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li><a href=\"#\" onclick=\"set\_ca\_id('{$row['ca\_id']}'); return false;\">{$row['ca\_name']} (".$row['cnt'].")</a></li>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div>'.$error.'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_paging($config['cf\_write\_pages'], $page, $total\_page, $\_SERVER['SCRIPT\_NAME'].'?'.$query\_string.'&amp;page=');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fregisterform" id="fregisterform" action="<?php echo $register\_action\_url; ?>" onsubmit="return fregisterform\_submit(this);" method="POST" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea readonly><?php echo get\_text($config['cf\_stipulation']) ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td>아이디, 이름, 비밀번호<?php echo ($config['cf\_cert\_use']) ? ", 생년월일, 휴대폰 번호(본인인증 할 때만, 아이핀 제외), 암호화된 개인식별부호(CI)" : ""; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="provider" value="<?php echo $provider\_name; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cert\_type" value="<?php echo $member['mb\_certify']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $user\_id; ?>" id="reg\_mb\_id">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="reg\_mb\_name" name="mb\_name" value="<?php echo $user\_name ? $user\_name : $user\_nick ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_hp" value="<?php echo get\_text($user\_phone); ?>" id="reg\_mb\_hp">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="old\_mb\_hp" value="<?php echo get\_text($user\_phone); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="tooltip">공백없이 한글,영문,숫자만 입력 가능 (한글2자, 영문4자 이상)<br> 닉네임을 바꾸시면 앞으로 <?php echo (int)$config['cf\_nick\_modify'] ?>일 이내에는 변경 할 수 없습니다.</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_nick\_default" value="<?php echo isset($user\_nick) ? get\_text($user\_nick) : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_nick" value="<?php echo isset($user\_nick) ? get\_text($user\_nick) : ''; ?>" id="reg\_mb\_nick" required class="frm\_input required nospace full\_input" size="10" maxlength="20" placeholder="닉네임">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="old\_email" value="<?php echo $member['mb\_email'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_email" value="<?php echo isset($user\_email) ? $user\_email : ''; ?>" id="reg\_mb\_email" required <?php echo (isset($user\_email) && $user\_email != '' && !$is\_exists\_email)? "readonly":''; ?> class="frm\_input email full\_input required" size="70" maxlength="100" placeholder="E-mail">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="check"><?php echo $email\_msg; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="submit" id="btn\_submit" class="btn\_submit" accesskey="s"><?php echo $w == '' ? '회원가입' : '정보수정'; ?></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 175 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form method="post" action="<?php echo $login\_action\_url ?>" onsubmit="return social\_obj.flogin\_submit(this);">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="url" name="url" value="<?php echo $login\_url ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="provider" name="provider" value="<?php echo $provider\_name ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 268 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_register\_member.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

certify\_win\_open("<?php echo $cert\_type; ?>", "<?php echo $cert\_url; ?>" + params);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_u\_register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $link\_href; ?>" id="sns-<?php echo $social; ?>" class="sns-icon social\_link sns-<?php echo $social; ?><?php echo $add\_class; ?>" title="<?php echo $title; ?>" data-provider="<?php echo $social; ?>" ><span class="ico"></span><span class="txt"><?php echo $provider\_name; ?> 로그인</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_u\_register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

socials["<?php echo $social; ?>"] = "<?php echo social\_nonce\_create($social, $session\_id); ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\social\social\_u\_register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

self\_url = "<?php echo $self\_url; ?>",

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><strong><?php echo number\_format($visit[1]) ?></strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><strong><?php echo number\_format($visit[2]) ?></strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><strong><?php echo number\_format($visit[3]) ?></strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><strong><?php echo number\_format($visit[4]) ?></strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == "super") { ?><a href="<?php echo G5\_ADMIN\_URL ?>/visit\_list.php" class="btn\_admin btn"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\visit\shop\_basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><strong><?php echo number\_format($visit[1]) ?></strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\visit\shop\_basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><strong><?php echo number\_format($visit[2]) ?></strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\visit\shop\_basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><strong><?php echo number\_format($visit[3]) ?></strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\visit\shop\_basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><strong><?php echo number\_format($visit[4]) ?></strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\skin\visit\shop\_basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == "super") { ?><a href="<?php echo G5\_ADMIN\_URL ?>/visit\_list.php" class="btn\_admin btn"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div style="float:left;<?php echo $lt\_style ?>" class="lt\_wr">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo latest('theme/basic', $row['bo\_table'], 6, 25);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="hd\_h1"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_URL ?>"><img src="<?php echo G5\_IMG\_URL ?>/logo.png" alt="<?php echo $config['cf\_title']; ?>"></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="gnb\_1dli <?php echo $add\_class; ?>" style="z-index:<?php echo $gnb\_zindex--; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $row['me\_link']; ?>" target="\_<?php echo $row['me\_target']; ?>" class="gnb\_1da"><?php echo $row['me\_name'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="gnb\_2dli"><a href="<?php echo $row2['me\_link']; ?>" target="\_<?php echo $row2['me\_target']; ?>" class="gnb\_2da"><?php echo $row2['me\_name'] ?></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="gnb\_empty">메뉴 준비 중입니다.<?php if ($is\_admin) { ?> <a href="<?php echo G5\_ADMIN\_URL; ?>/menu\_list.php">관리자모드 &gt; 환경설정 &gt; 메뉴설정</a>에서 설정하실 수 있습니다.<?php } ?></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $row['me\_link']; ?>" target="\_<?php echo $row['me\_target']; ?>" class="gnb\_al\_a"><?php echo $row['me\_name'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 172 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $row2['me\_link']; ?>" target="\_<?php echo $row2['me\_target']; ?>"><?php echo $row2['me\_name'] ?></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 186 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="gnb\_empty">메뉴 준비 중입니다.<?php if ($is\_admin) { ?> <br><a href="<?php echo G5\_ADMIN\_URL; ?>/menu\_list.php">관리자모드 &gt; 환경설정 &gt; 메뉴설정</a>에서 설정하실 수 있습니다.<?php } ?></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 217 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (!defined("\_INDEX\_")) { ?><h2 id="container\_title"><span title="<?php echo get\_text($g5['title']); ?>"><?php echo get\_head\_title($g5['title']); ?></span></h2><?php }

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $config['cf\_add\_meta'].PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<title><?php echo $g5\_head\_title; ?></title>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<link rel="stylesheet" href="'.run\_replace('head\_css\_url', G5\_THEME\_CSS\_URL.'/'.(G5\_IS\_MOBILE?'mobile':'default').$shop\_css.'.css?ver='.G5\_CSS\_VER, G5\_THEME\_URL).'">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var g5\_is\_member = "<?php echo isset($is\_member)?$is\_member:''; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var g5\_is\_admin = "<?php echo isset($is\_admin)?$is\_admin:''; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var g5\_bo\_table = "<?php echo isset($bo\_table)?$bo\_table:''; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var g5\_sca = "<?php echo isset($sca)?$sca:''; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var g5\_editor = "<?php echo ($config['cf\_editor'] && $board['bo\_use\_dhtml\_editor'])?$config['cf\_editor']:''; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $config['cf\_add\_script'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<body<?php echo isset($g5['body\_script']) ? $g5['body\_script'] : ''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\head.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="hd\_login\_msg">'.$sr\_admin\_msg.get\_text($member['mb\_nick']).'님 로그인 중 ';

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\index.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

from `{$g5['board\_table']}` a left join `{$g5['group\_table']}` b on (a.gr\_id=b.gr\_id)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div style="float:left;<?php echo $lt\_style ?>" class="lt\_wr">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo latest('theme/basic', $row['bo\_table'], 6, 24);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $config['cf\_analytics'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 5 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\tail.sub.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == 'super') { ?><!-- <div style='float:left; text-align:center;'>RUN TIME : <?php echo get\_microtime()-$begin\_time; ?><br></div> --><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\group.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo latest('theme/basic', $row['bo\_table'], 5, 70);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="hd\_h1"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_URL ?>"><img src="<?php echo G5\_IMG\_URL ?>/m\_logo.png" alt="<?php echo $config['cf\_title']; ?>"></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $row['me\_link']; ?>" target="\_<?php echo $row['me\_target']; ?>" class="gnb\_1da"><?php echo $row['me\_name'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="gnb\_2dli"><a href="<?php echo $row2['me\_link']; ?>" target="\_<?php echo $row2['me\_target']; ?>" class="gnb\_2da"><span></span><?php echo $row2['me\_name'] ?></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li id="gnb\_empty">메뉴 준비 중입니다.<?php if ($is\_admin) { ?> <br><a href="<?php echo G5\_ADMIN\_URL; ?>/menu\_list.php">관리자모드 &gt; 환경설정 &gt; 메뉴설정</a>에서 설정하세요.<?php } ?></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 190 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 id="container\_title" class="top" title="<?php echo get\_text($g5['title']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 191 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:history.back();"><i class="fa fa-chevron-left" aria-hidden="true"></i><span class="sound\_only">뒤로가기</span></a> <?php echo get\_head\_title($g5['title']); ?>

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\index.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

from `{$g5['board\_table']}` a left join `{$g5['group\_table']}` b on (a.gr\_id=b.gr\_id)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo latest('theme/basic', $row['bo\_table'], 12, 25);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $config['cf\_analytics'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $mshop\_ca\_row1['url']; ?>"><?php echo get\_text($mshop\_ca\_row1['ca\_name']); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<button class="sub\_ct\_toggle ct\_op">'.get\_text($mshop\_ca\_row1['ca\_name']).' 하위분류 열기</button>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $mshop\_ca\_row2['url']; ?>"><?php echo get\_text($mshop\_ca\_row2['ca\_name']); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<button type="button" class="sub\_ct\_toggle ct\_op">'.get\_text($mshop\_ca\_row2['ca\_name']).' 하위분류 열기</button>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $mshop\_ca\_row3['url']; ?>"><?php echo get\_text($mshop\_ca\_row3['ca\_name']); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<button type="button" class="sub\_ct\_toggle ct\_op">'.get\_text($mshop\_ca\_row3['ca\_name']).' 하위분류 열기</button>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo shop\_category\_url($mshop\_ca\_row4['ca\_id']); ?>"><?php echo get\_text($mshop\_ca\_row4['ca\_name']); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<button type="button" class="sub\_ct\_toggle ct\_op">'.get\_text($mshop\_ca\_row4['ca\_name']).' 하위분류 열기</button>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo shop\_category\_url($mshop\_ca\_row5['ca\_id']); ?>"><?php echo get\_text($mshop\_ca\_row5['ca\_name']); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ((!$bo\_table || $w == 's' ) && defined('\_INDEX\_')) { ?><h1><?php echo $config['cf\_title'] ?></h1><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="logo"><a href="<?php echo G5\_SHOP\_URL; ?>/"><img src="<?php echo G5\_DATA\_URL; ?>/common/mobile\_logo\_img" alt="<?php echo $config['cf\_title']; ?> 메인"></a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="q" value="<?php echo stripslashes(get\_text(get\_search\_string($q))); ?>" id="sch\_str" required class="frm\_input" placeholder="검색어를 입력해주세요">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="container" class="<?php echo implode(' ', $container\_class); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ((!$bo\_table || $w == 's' ) && !defined('\_INDEX\_')) { ?><h1 id="container\_title"><a href="javascript:history.back()" class="btn\_back"><i class="fa fa-chevron-left" aria-hidden="true"></i><span class="sound\_only">뒤로</span></a> <?php echo $g5['title'] ?></h1><?php }

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $config['cf\_title']; ?> 정보</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="ft\_logo"><a href="<?php echo G5\_SHOP\_URL; ?>/"><img src="<?php echo G5\_DATA\_URL; ?>/common/mobile\_logo\_img2" alt="<?php echo $config['cf\_title']; ?> 메인"></a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>회사명</b> <?php echo $default['de\_admin\_company\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>주소</b> <?php echo $default['de\_admin\_company\_addr']; ?></span><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>사업자 등록번호</b> <?php echo $default['de\_admin\_company\_saupja\_no']; ?></span><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>대표</b> <?php echo $default['de\_admin\_company\_owner']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>전화</b> <?php echo $default['de\_admin\_company\_tel']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>팩스</b> <?php echo $default['de\_admin\_company\_fax']; ?></span><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <span><b>운영자</b> <?php echo $admin['mb\_name']; ?></span><br> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>통신판매업신고번호</b> <?php echo $default['de\_admin\_tongsin\_no']; ?></span><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>개인정보 보호책임자</b> <?php echo $default['de\_admin\_info\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($default['de\_admin\_buga\_no']) echo '<span><b>부가통신사업신고번호</b> '.$default['de\_admin\_buga\_no'].'</span>'; ?><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

Copyright &copy; 2001-2013 <?php echo $default['de\_admin\_company\_name']; ?>. All Rights Reserved.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $config['cf\_analytics'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<ul class="<?php echo isset($view) ? 'view\_is\_list btn\_top' : 'btn\_top top btn\_bo\_user';?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($admin\_href) { ?><li><a href="<?php echo $admin\_href ?>" class="btn\_admin btn" title="관리자"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($rss\_href) { ?><li><a href="<?php echo $rss\_href ?>" class="btn\_b03 btn" title="RSS"><i class="fa fa-rss" aria-hidden="true"></i><span class="sound\_only">RSS</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="fix\_btn write\_btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo ($board['bo\_mobile\_subject'] ? $board['bo\_mobile\_subject'] : $board['bo\_subject']) ?> 카테고리</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php if ($list[$i]['is\_notice']) echo "bo\_notice"; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_wr\_id[]" value="<?php echo $list[$i]['wr\_id'] ?>" id="chk\_wr\_id\_<?php echo $i ?>" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_wr\_id\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<b class="sound\_only"><?php echo $list[$i]['subject'] ?></b>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['ca\_name\_href'] ?>" class="bo\_cate\_link"><?php echo $list[$i]['ca\_name']; ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['href'] ?>" class="bo\_subject">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['icon\_reply']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (isset($list[$i]['icon\_secret'])) echo $list[$i]['icon\_secret']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['subject'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_hot'])) echo $list[$i]['icon\_hot'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_file'])) echo $list[$i]['icon\_file'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_link'])) echo $list[$i]['icon\_link'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['comment\_cnt']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자</span><?php echo $list[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_date"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$i]['datetime2'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_view"><i class="fa fa-eye" aria-hidden="true"></i> <?php echo number\_format($list[$i]['wr\_hit']) ?><span class="sound\_only">회</span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_good) { ?><span class="sound\_only">추천</span><i class="fa fa-thumbs-o-up" aria-hidden="true"></i> <?php echo $list[$i]['wr\_good'] ?><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_nogood) { ?><span class="sound\_only">비추천</span><i class="fa fa-thumbs-o-down" aria-hidden="true"></i> <?php echo $list[$i]['wr\_nogood'] ?><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (count($list) == 0) { echo '<li class="empty\_table">게시물이 없습니다.</li>'; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>전체 <?php echo number\_format($total\_count) ?>건</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $page ?> 페이지

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_board\_sfl\_select\_options($sfl); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input name="stx" value="<?php echo stripslashes($stx) ?>" placeholder="검색어를 입력하세요" required id="stx" class="sch\_input" size="15" maxlength="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- 게시판 이름 표시 <div id="bo\_v\_table"><?php echo ($board['bo\_mobile\_subject'] ? $board['bo\_mobile\_subject'] : $board['bo\_subject']); ?></div> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($scrap\_href) { ?><a href="<?php echo $scrap\_href; ?>" target="\_blank" class=" btn\_scrap" onclick="win\_scrap(this.href); return false;" title="스크랩"><i class="fa fa-thumb-tack" aria-hidden="true"></i><span class="sound\_only">스크랩</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b03 btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($reply\_href) { ?><li><a href="<?php echo $reply\_href ?>"><i class="fa fa-reply" aria-hidden="true"></i> 답변</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($update\_href) { ?><li><a href="<?php echo $update\_href ?>"><i class="fa fa-pencil-square-o" aria-hidden="true"></i> 수정</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($delete\_href) { ?><li><a href="<?php echo $delete\_href ?>" onclick="del(this.href); return false;"><i class="fa fa-trash-o" aria-hidden="true"></i> 삭제</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($copy\_href) { ?><li><a href="<?php echo $copy\_href ?>" onclick="board\_move(this.href); return false;"><i class="fa fa-files-o" aria-hidden="true"></i> 복사</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($move\_href) { ?><li><a href="<?php echo $move\_href ?>" onclick="board\_move(this.href); return false;"><i class="fa fa-arrows" aria-hidden="true"></i> 이동</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($search\_href) { ?><li><a href="<?php echo $search\_href ?>">검색</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $list\_href ?>" class="btn\_list"><i class="fa fa-list" aria-hidden="true"></i> 목록</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="bo\_v" style="width:<?php echo $width; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_cate"><?php echo $view['ca\_name'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_tit"><?php echo cut\_str(get\_text($view['wr\_subject']), 70);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자 </span><?php echo $view['name'] ?><span class="ip"><?php if ($is\_ip\_view) { echo "&nbsp;($ip)"; } ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성일</span><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo date("y-m-d H:i", strtotime($view['wr\_datetime'])) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">조회</span><strong><i class="fa fa-eye" aria-hidden="true"></i> <?php echo number\_format($view['wr\_hit']) ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">댓글</span><strong><i class="fa fa-commenting-o" aria-hidden="true"></i> <?php echo number\_format($view['wr\_comment']) ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_file\_thumbnail($view\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="bo\_v\_con"><?php echo get\_view\_thumbnail($view['content']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_signature) { ?><p><?php echo $signature ?></p><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $good\_href.'&amp;'.$qstr ?>" id="good\_button" class="bo\_v\_good"><i class="fa fa-thumbs-o-up" aria-hidden="true"></i> <span class="sound\_only">추천</span><strong><?php echo number\_format($view['wr\_good']) ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $nogood\_href.'&amp;'.$qstr ?>" id="nogood\_button" class="bo\_v\_nogood"><i class="fa fa-thumbs-o-down" aria-hidden="true"></i> <span class="sound\_only">비추천</span><strong><?php echo number\_format($view['wr\_nogood']) ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($board['bo\_use\_good']) { ?><span class="bo\_v\_good"><i class="fa fa-thumbs-o-up" aria-hidden="true"></i><span class="sound\_only">추천</span><strong><?php echo number\_format($view['wr\_good']) ?></strong></span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($board['bo\_use\_nogood']) { ?><span class="bo\_v\_nogood"><i class="fa fa-thumbs-o-down" aria-hidden="true"></i><span class="sound\_only">비추천</span> <strong><?php echo number\_format($view['wr\_nogood']) ?></strong></span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['file'][$i]['href']; ?>" class="view\_file\_download">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $view['file'][$i]['source'] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $view['file'][$i]['content'] ?> (<?php echo $view['file'][$i]['size'] ?>)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_file\_cnt"><?php echo $view['file'][$i]['download'] ?>회 다운로드</span> |

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>DATE : <?php echo $view['file'][$i]['datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['link\_href'][$i] ?>" target="\_blank">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $link ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_link\_cnt"><?php echo $view['link\_hit'][$i] ?>회 연결</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 193 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($prev\_href) { ?><li class="bo\_v\_prev"><a href="<?php echo $prev\_href ?>"><i class="fa fa-chevron-up" aria-hidden="true"></i><span class="sound\_only">이전글</span> <?php echo $prev\_wr\_subject;?></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 194 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($next\_href) { ?><li class="bo\_v\_next"><a href="<?php echo $next\_href ?>"><i class="fa fa-chevron-down" aria-hidden="true"></i><span class="sound\_only">다음글</span> <?php echo $next\_wr\_subject;?></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 214 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var msg = "파일을 다운로드 하시면 포인트가 차감(<?php echo number\_format($board['bo\_download\_point']) ?>점)됩니다.\n\n포인트는 게시물당 한번만 차감되며 다음에 다시 다운로드 하셔도 중복하여 차감하지 않습니다.\n\n그래도 다운로드 하시겠습니까?";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_min = parseInt(<?php echo $comment\_min ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_max = parseInt(<?php echo $comment\_max ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="bo\_vc\_tit">댓글목록 <span><?php echo $view['wr\_comment']; ?></span></h2>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace("/\[\<a\s.\*href\=\"(http|https|ftp|mms)\:\/\/([^[:space:]]+)\.(mp3|wma|wmv|asf|asx|mpg|mpeg)\".\*\<\/a\>\]/i", "<script>doc\_write(obj\_movie('$1:

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="c\_<?php echo $comment\_id ?>" <?php if ($cmt\_depth) { ?>style="margin-left:<?php echo $cmt\_depth ?>px;border-bottom-color:#f8f8f8"<?php } ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo get\_text($list[$i]['wr\_name']); ?>님의 댓글<?php if ($cmt\_depth) { ?><span class="sound\_only">의 댓글</span><?php } ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_vc\_hdinfo">(<?php echo $list[$i]['ip']; ?>)</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_vc\_hdinfo"><i class="fa fa-clock-o" aria-hidden="true"></i> <time datetime="<?php echo date('Y-m-d\TH:i:s+09:00', strtotime($list[$i]['datetime'])) ?>"><?php echo $list[$i]['datetime'] ?></time></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_reply']) { ?><li><a href="<?php echo $c\_reply\_href; ?>" onclick="comment\_box('<?php echo $comment\_id ?>', 'c'); return false;">답변</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_edit']) { ?><li><a href="<?php echo $c\_edit\_href; ?>" onclick="comment\_box('<?php echo $comment\_id ?>', 'cu'); return false;">수정</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_del']) { ?><li><a href="<?php echo $list[$i]['del\_link']; ?>" onclick="return comment\_delete();">삭제</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (strstr($list[$i]['wr\_option'], "secret")) echo "<img src=\"".$board\_skin\_url."/img/icon\_secret.gif\" alt=\"비밀글\">"; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="edit\_<?php echo $comment\_id ?>"></span><!-- 수정 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="reply\_<?php echo $comment\_id ?>"></span><!-- 답변 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="secret\_comment\_<?php echo $comment\_id ?>" value="<?php echo strstr($list[$i]['wr\_option'],"secret") ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea id="save\_comment\_<?php echo $comment\_id ?>" style="display:none"><?php echo get\_text($list[$i]['content1'], 0) ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fviewcomment" id="fviewcomment" action="<?php echo $comment\_action\_url; ?>" onsubmit="return fviewcomment\_submit(this);" method="post" autocomplete="off" class="bo\_vc\_w">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>" id="w">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comment\_id" value="<?php echo $c\_id ?>" id="comment\_id">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($comment\_min || $comment\_max) { ?>onkeyup="check\_byte('wr\_content', 'char\_count');"<?php } ?> placeholder="댓글내용을 입력해주세요"><?php echo $c\_wr\_content; ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_html; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 254 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($is\_guest) echo chk\_captcha\_js(); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 325 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

"<?php echo G5\_SNS\_URL; ?>/view\_comment\_write.sns.skin.php?bo\_table=<?php echo $bo\_table; ?>",

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fwrite" id="fwrite" action="<?php echo $action\_url ?>" onsubmit="return fwrite\_submit(this);" method="post" enctype="multipart/form-data" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_hidden;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="sound\_only"><?php echo $g5['title'] ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_name" value="<?php echo $name ?>" id="wr\_name" required class="frm\_input full\_input required" maxlength="20" placeholder="이름">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="password" name="wr\_password" id="wr\_password" <?php echo $password\_required ?> class="frm\_input full\_input <?php echo $password\_required ?>" maxlength="20" placeholder="비밀번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="email" name="wr\_email" value="<?php echo $email ?>" id="wr\_email" class="frm\_input full\_input" maxlength="100" placeholder="이메일">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_homepage" value="<?php echo $homepage ?>" id="wr\_homepage" class="frm\_input full\_input" placeholder="홈페이지">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_subject" value="<?php echo $subject ?>" id="wr\_subject" required class="frm\_input full\_input required" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p id="char\_count\_desc">이 게시판은 최소 <strong><?php echo $write\_min; ?></strong>글자 이상, 최대 <strong><?php echo $write\_max; ?></strong>글자 이하까지 글을 쓰실 수 있습니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="wr\_link<?php echo $i ?>"><i class="fa fa-link" aria-hidden="true"></i> <span class="sound\_only">링크 #<?php echo $i ?></span></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_link<?php echo $i ?>" value="<?php if($w=="u"){echo $write['wr\_link'.$i];} ?>" id="wr\_link<?php echo $i ?>" class="frm\_input wr\_link" placeholder="링크를 입력하세요">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bf\_file\_<?php echo $i+1 ?>"><i class="fa fa-download lb\_icon" aria-hidden="true"></i><span class="sound\_only">파일 #<?php echo $i+1 ?></span><span class="btn\_file">파일첨부</span></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="file" name="bf\_file[]" id="bf\_file\_<?php echo $i+1 ?>" title="파일첨부 <?php echo $i+1 ?> : 용량 <?php echo $upload\_max\_filesize ?> 이하만 업로드 가능" class="frm\_file uploadBtn">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bf\_content[]" value="<?php echo ($w == 'u') ? $file[$i]['bf\_content'] : ''; ?>" title="파일 설명을 입력해주세요." class="full\_input frm\_input" size="50" placeholder="파일 설명을 입력해주세요.">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="bf\_file\_del<?php echo $i ?>" name="bf\_file\_del[<?php echo $i; ?>]" value="1"> <label for="bf\_file\_del<?php echo $i ?>"><?php echo $file[$i]['source'].'('.$file[$i]['size'].')'; ?> 파일 삭제</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_html ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="btn\_cancel">취소</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_min = parseInt(<?php echo $write\_min; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_max = parseInt(<?php echo $write\_max; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<ul class="<?php echo isset($view) ? 'view\_is\_list btn\_top' : 'btn\_top top btn\_bo\_user';?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($admin\_href) { ?><li><a href="<?php echo $admin\_href ?>" class="btn\_admin btn" title="관리자"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($rss\_href) { ?><li><a href="<?php echo $rss\_href ?>" class="btn\_b03 btn" title="RSS"><i class="fa fa-rss" aria-hidden="true"></i><span class="sound\_only">RSS</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="fix\_btn write\_btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo ($board['bo\_mobile\_subject'] ? $board['bo\_mobile\_subject'] : $board['bo\_subject']) ?> 카테고리</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_wr\_id[]" value="<?php echo $list[$i]['wr\_id'] ?>" id="chk\_wr\_id\_<?php echo $i ?>" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_wr\_id\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<b class="sound\_only"><?php echo $list[$i]['subject'] ?></b>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['num'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['href'] ?>" class="gall\_img">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo run\_replace('thumb\_image\_tag', $img\_content, $thumb);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['ca\_name\_href'] ?>" class="bo\_cate\_link"><?php echo $list[$i]['ca\_name'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['href'] ?>" class="gall\_li\_tit">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (isset($list[$i]['icon\_secret'])) echo $list[$i]['icon\_secret']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['subject'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['comment\_cnt']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_hot'])) echo $list[$i]['icon\_hot'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자 </span><?php echo $list[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성일 </span><span class="date"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$i]['datetime2'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">조회 </span><strong><i class="fa fa-eye" aria-hidden="true"></i> <?php echo $list[$i]['wr\_hit'] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_good) { ?><span class="sound\_only">추천</span><strong><i class="fa fa-thumbs-o-up" aria-hidden="true"></i> <?php echo $list[$i]['wr\_good'] ?></strong><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_nogood) { ?><span class="sound\_only">비추천</span><strong><i class="fa fa-thumbs-o-down" aria-hidden="true"></i> <?php echo $list[$i]['wr\_nogood'] ?></strong><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (count($list) == 0) { echo "<li class=\"empty\_list\">게시물이 없습니다.</li>"; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>전체 <?php echo number\_format($total\_count) ?>건</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 160 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $page ?> 페이지

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_board\_sfl\_select\_options($sfl); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input name="stx" value="<?php echo stripslashes($stx) ?>" placeholder="검색어를 입력하세요" required id="stx" class="sch\_input" size="15" maxlength="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- 게시판 이름 표시 <div id="bo\_v\_table"><?php echo ($board['bo\_mobile\_subject'] ? $board['bo\_mobile\_subject'] : $board['bo\_subject']); ?></div> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($scrap\_href) { ?><a href="<?php echo $scrap\_href; ?>" target="\_blank" class=" btn\_scrap" onclick="win\_scrap(this.href); return false;" title="스크랩"><i class="fa fa-thumb-tack" aria-hidden="true"></i><span class="sound\_only">스크랩</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b03 btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($reply\_href) { ?><li><a href="<?php echo $reply\_href ?>"><i class="fa fa-reply" aria-hidden="true"></i> 답변</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($update\_href) { ?><li><a href="<?php echo $update\_href ?>"><i class="fa fa-pencil-square-o" aria-hidden="true"></i> 수정</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($delete\_href) { ?><li><a href="<?php echo $delete\_href ?>" onclick="del(this.href); return false;"><i class="fa fa-trash-o" aria-hidden="true"></i> 삭제</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($copy\_href) { ?><li><a href="<?php echo $copy\_href ?>" onclick="board\_move(this.href); return false;"><i class="fa fa-files-o" aria-hidden="true"></i> 복사</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($move\_href) { ?><li><a href="<?php echo $move\_href ?>" onclick="board\_move(this.href); return false;"><i class="fa fa-arrows" aria-hidden="true"></i> 이동</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($search\_href) { ?><li><a href="<?php echo $search\_href ?>">검색</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $list\_href ?>" class="btn\_list"><i class="fa fa-list" aria-hidden="true"></i> 목록</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="bo\_v" style="width:<?php echo $width; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_cate"><?php echo $view['ca\_name'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_tit"><?php echo cut\_str(get\_text($view['wr\_subject']), 70);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자 </span><?php echo $view['name'] ?><span class="ip"><?php if ($is\_ip\_view) { echo "&nbsp;($ip)"; } ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성일</span><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo date("y-m-d H:i", strtotime($view['wr\_datetime'])) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">조회</span><strong><i class="fa fa-eye" aria-hidden="true"></i> <?php echo number\_format($view['wr\_hit']) ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">댓글</span><strong><i class="fa fa-commenting-o" aria-hidden="true"></i> <?php echo number\_format($view['wr\_comment']) ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_file\_thumbnail($view\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="bo\_v\_con"><?php echo get\_view\_thumbnail($view['content']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_signature) { ?><p><?php echo $signature ?></p><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $good\_href.'&amp;'.$qstr ?>" id="good\_button" class="bo\_v\_good"><i class="fa fa-thumbs-o-up" aria-hidden="true"></i> <span class="sound\_only">추천</span><strong><?php echo number\_format($view['wr\_good']) ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $nogood\_href.'&amp;'.$qstr ?>" id="nogood\_button" class="bo\_v\_nogood"><i class="fa fa-thumbs-o-down" aria-hidden="true"></i> <span class="sound\_only">비추천</span><strong><?php echo number\_format($view['wr\_nogood']) ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($board['bo\_use\_good']) { ?><span class="bo\_v\_good"><i class="fa fa-thumbs-o-up" aria-hidden="true"></i><span class="sound\_only">추천</span><strong><?php echo number\_format($view['wr\_good']) ?></strong></span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($board['bo\_use\_nogood']) { ?><span class="bo\_v\_nogood"><i class="fa fa-thumbs-o-down" aria-hidden="true"></i><span class="sound\_only">비추천</span> <strong><?php echo number\_format($view['wr\_nogood']) ?></strong></span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['file'][$i]['href']; ?>" class="view\_file\_download">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $view['file'][$i]['source'] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $view['file'][$i]['content'] ?> (<?php echo $view['file'][$i]['size'] ?>)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_file\_cnt"><?php echo $view['file'][$i]['download'] ?>회 다운로드</span> |

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>DATE : <?php echo $view['file'][$i]['datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['link\_href'][$i] ?>" target="\_blank">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $link ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 182 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_link\_cnt"><?php echo $view['link\_hit'][$i] ?>회 연결</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($prev\_href) { ?><li class="bo\_v\_prev"><a href="<?php echo $prev\_href ?>"><i class="fa fa-chevron-up" aria-hidden="true"></i><span class="sound\_only">이전글</span> <?php echo $prev\_wr\_subject;?></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 196 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($next\_href) { ?><li class="bo\_v\_next"><a href="<?php echo $next\_href ?>"><i class="fa fa-chevron-down" aria-hidden="true"></i><span class="sound\_only">다음글</span> <?php echo $next\_wr\_subject;?></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 215 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var msg = "파일을 다운로드 하시면 포인트가 차감(<?php echo number\_format($board['bo\_download\_point']) ?>점)됩니다.\n\n포인트는 게시물당 한번만 차감되며 다음에 다시 다운로드 하셔도 중복하여 차감하지 않습니다.\n\n그래도 다운로드 하시겠습니까?";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_min = parseInt(<?php echo $comment\_min ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_max = parseInt(<?php echo $comment\_max ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="bo\_vc\_tit">댓글목록 <span><?php echo $view['wr\_comment']; ?></span></h2>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$str = preg\_replace("/\[\<a\s.\*href\=\"(http|https|ftp|mms)\:\/\/([^[:space:]]+)\.(mp3|wma|wmv|asf|asx|mpg|mpeg)\".\*\<\/a\>\]/i", "<script>doc\_write(obj\_movie('$1:

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="c\_<?php echo $comment\_id ?>" <?php if ($cmt\_depth) { ?>style="margin-left:<?php echo $cmt\_depth ?>px;border-bottom-color:#f8f8f8"<?php } ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo get\_text($list[$i]['wr\_name']); ?>님의 댓글<?php if ($cmt\_depth) { ?><span class="sound\_only">의 댓글</span><?php } ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_vc\_hdinfo">(<?php echo $list[$i]['ip']; ?>)</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_vc\_hdinfo"><i class="fa fa-clock-o" aria-hidden="true"></i> <time datetime="<?php echo date('Y-m-d\TH:i:s+09:00', strtotime($list[$i]['datetime'])) ?>"><?php echo $list[$i]['datetime'] ?></time></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_reply']) { ?><li><a href="<?php echo $c\_reply\_href; ?>" onclick="comment\_box('<?php echo $comment\_id ?>', 'c'); return false;">답변</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_edit']) { ?><li><a href="<?php echo $c\_edit\_href; ?>" onclick="comment\_box('<?php echo $comment\_id ?>', 'cu'); return false;">수정</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_del']) { ?><li><a href="<?php echo $list[$i]['del\_link']; ?>" onclick="return comment\_delete();">삭제</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (strstr($list[$i]['wr\_option'], "secret")) echo "<img src=\"".$board\_skin\_url."/img/icon\_secret.gif\" alt=\"비밀글\">"; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="edit\_<?php echo $comment\_id ?>"></span><!-- 수정 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="reply\_<?php echo $comment\_id ?>"></span><!-- 답변 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="secret\_comment\_<?php echo $comment\_id ?>" value="<?php echo strstr($list[$i]['wr\_option'],"secret") ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea id="save\_comment\_<?php echo $comment\_id ?>" style="display:none"><?php echo get\_text($list[$i]['content1'], 0) ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fviewcomment" id="fviewcomment" action="<?php echo $comment\_action\_url; ?>" onsubmit="return fviewcomment\_submit(this);" method="post" autocomplete="off" class="bo\_vc\_w">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>" id="w">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comment\_id" value="<?php echo $c\_id ?>" id="comment\_id">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($comment\_min || $comment\_max) { ?>onkeyup="check\_byte('wr\_content', 'char\_count');"<?php } ?> placeholder="댓글내용을 입력해주세요"><?php echo $c\_wr\_content; ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_html; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 254 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($is\_guest) echo chk\_captcha\_js(); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 325 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

"<?php echo G5\_SNS\_URL; ?>/view\_comment\_write.sns.skin.php?bo\_table=<?php echo $bo\_table; ?>",

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fwrite" id="fwrite" action="<?php echo $action\_url ?>" onsubmit="return fwrite\_submit(this);" method="post" enctype="multipart/form-data" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_hidden;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="sound\_only"><?php echo $g5['title'] ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_name" value="<?php echo $name ?>" id="wr\_name" required class="frm\_input full\_input required" maxlength="20" placeholder="이름">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="password" name="wr\_password" id="wr\_password" <?php echo $password\_required ?> class="frm\_input full\_input <?php echo $password\_required ?>" maxlength="20" placeholder="비밀번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="email" name="wr\_email" value="<?php echo $email ?>" id="wr\_email" class="frm\_input full\_input" maxlength="100" placeholder="이메일">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_homepage" value="<?php echo $homepage ?>" id="wr\_homepage" class="frm\_input full\_input" placeholder="홈페이지">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_subject" value="<?php echo $subject ?>" id="wr\_subject" required class="frm\_input full\_input required" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p id="char\_count\_desc">이 게시판은 최소 <strong><?php echo $write\_min; ?></strong>글자 이상, 최대 <strong><?php echo $write\_max; ?></strong>글자 이하까지 글을 쓰실 수 있습니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="wr\_link<?php echo $i ?>"><i class="fa fa-link" aria-hidden="true"></i> <span class="sound\_only">링크 #<?php echo $i ?></span></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_link<?php echo $i ?>" value="<?php if($w=="u"){echo $write['wr\_link'.$i];} ?>" id="wr\_link<?php echo $i ?>" class="frm\_input wr\_link" placeholder="링크를 입력하세요">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bf\_file\_<?php echo $i+1 ?>"><i class="fa fa-download lb\_icon" aria-hidden="true"></i><span class="sound\_only">파일 #<?php echo $i+1 ?></span><span class="btn\_file">파일첨부</span></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="file" name="bf\_file[]" id="bf\_file\_<?php echo $i+1 ?>" title="파일첨부 <?php echo $i+1 ?> : 용량 <?php echo $upload\_max\_filesize ?> 이하만 업로드 가능" class="frm\_file uploadBtn">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bf\_content[]" value="<?php echo ($w == 'u') ? $file[$i]['bf\_content'] : ''; ?>" title="파일 설명을 입력해주세요." class="full\_input frm\_input" size="50" placeholder="파일 설명을 입력해주세요.">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="bf\_file\_del<?php echo $i ?>" name="bf\_file\_del[<?php echo $i; ?>]" value="1"> <label for="bf\_file\_del<?php echo $i ?>"><?php echo $file[$i]['source'].'('.$file[$i]['size'].')'; ?> 파일 삭제</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_html ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="btn\_cancel">취소</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_min = parseInt(<?php echo $write\_min; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_max = parseInt(<?php echo $write\_max; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\connect\basic\connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $row['total\_cnt'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\connect\basic\current\_connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="crt\_num"><?php echo $list[$i]['num'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\connect\basic\current\_connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="crt\_profile"><?php echo get\_member\_profile\_img($list[$i]['mb\_id']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\connect\basic\current\_connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="crt\_name"><?php echo $list[$i]['name'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\connect\basic\current\_connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="crt\_lct"><?php echo $display\_location ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\content\basic\content.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="ctt" class="ctt\_<?php echo $co\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\content\basic\content.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title']; ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\content\basic\content.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="faq\_hhtml">'.conv\_content($fm['fm\_mobile\_head\_html'], 1).'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fm\_id" value="<?php echo $fm\_id;?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx;?>" required id="stx" class="frm\_input" size="15" maxlength="15">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $category\_href;?>?fm\_id=<?php echo $v['fm\_id']?>" <?php echo $category\_option;?> ><?php echo $category\_msg.$v['fm\_subject'];?></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="faq\_wrap" class="faq\_<?php echo $fm\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $g5['title']; ?> 목록</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="tit\_bg">Q</span><a href="#none" onclick="return faq\_open(this);"><?php echo conv\_content($v['fa\_subject'], 1); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($v['fa\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($page\_rows, $page, $total\_page, $\_SERVER['SCRIPT\_NAME'].'?'.$qstr.'&amp;page='); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="faq\_thtml">'.conv\_content($fm['fm\_mobile\_tail\_html'], 1).'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="lt\_title"><strong><?php echo $bo\_subject; ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="<?php echo $list\_count ? 'latest-sel' : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $echo\_ul;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".$wr\_href."\" class=\"lt\_thumb\">".run\_replace('thumb\_image\_tag', $img\_content, $thumb)."</a> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".$wr\_href."\" class=\"lt\_tit\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_secret']) echo "<i class=\"fa fa-lock\" aria-hidden=\"true\"></i> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strong>".$list[$i]['subject']."</strong>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo " <span class=\"new\_icon\">N</span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_file']) echo " <i class=\"fa fa-download\" aria-hidden=\"true\"></i>" ;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_link']) echo " <i class=\"fa fa-link\" aria-hidden=\"true\"></i>" ;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_hot']) echo " <i class=\"fa fa-heart\" aria-hidden=\"true\"></i>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['comment\_cnt']) echo "

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['datetime'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="page\_print"><b><?php echo $start\_page\_num; ?></b>/<?php echo $start\_page\_num; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="lt\_more"><span class="sound\_only"><?php echo $bo\_subject ?></span>전체보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\comment\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="cm\_lt\_title"><a href="<?php echo get\_pretty\_url($bo\_table); ?>">최신댓글</a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\comment\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="cm\_lt\_nick"><?php echo get\_member\_profile\_img($member['mb\_id']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\comment\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table, $list[$i]['wr\_id']); ?>" class="over"><?php echo $list[$i]['subject']; ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\comment\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="lt\_nick"><?php echo $list[$i]['name'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\comment\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="lt\_date"><?php echo $list[$i]['datetime2'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\comment\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="lt\_more"><span class="sound\_only"><?php echo $bo\_subject ?></span>더보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><a href="<?php echo get\_pretty\_url($bo\_table); ?>"><?php echo $bo\_subject ?></a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_secret']) echo "<span class=\"lock\_icon\"><i class=\"fa fa-lock\" aria-hidden=\"true\"></i></span> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".get\_pretty\_url($bo\_table, $list[$i]['wr\_id'])."\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strong>".$list[$i]['subject']."</strong>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['comment\_cnt'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><a href="<?php echo G5\_BBS\_URL ?>/board.php?bo\_table=<?php echo $bo\_table ?>"><?php echo $bo\_subject ?></a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".$list[$i]['href']."\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strong>".$list[$i]['subject']."</strong>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_new'])) echo " " . $list[$i]['icon\_new'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_BBS\_URL ?>/board.php?bo\_table=<?php echo $bo\_table ?>" class="more\_btn"><span class="sound\_only"><?php echo $bo\_subject ?></span>전체보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\formmail.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $name ?>님께 메일보내기</h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\formmail.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="to" value="<?php echo $email ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\formmail.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fnick" value="<?php echo get\_text($member['mb\_nick']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\formmail.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fmail" value="<?php echo $member['mb\_email'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="flogin" action="<?php echo $login\_action\_url ?>" onsubmit="return flogin\_submit(this);" method="post" id="flogin">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="url" value="<?php echo $login\_url ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $default['de\_guest\_privacy']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

f.url.value = "<?php echo $url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

f.action = "<?php echo $url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="forderinquiry" method="post" action="<?php echo urldecode($url); ?>" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_id" value="<?php echo $od\_id ?>" id="od\_id" placeholder="주문번호" required class="frm\_input required" size="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fcertrefreshform" id="member\_cert\_refresh" action="<?php echo $action\_url ?>" onsubmit="return fcertrefreshform\_submit(this);" method="POST" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cert\_type" value="<?php echo $member['mb\_certify']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $member['mb\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_hp" value="<?php echo $member['mb\_hp']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_name" value="<?php echo $member['mb\_name']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td>생년월일<?php echo (empty($member['mb\_dupinfo']))? ", 휴대폰 번호(아이핀 제외)" : ""; ?>, 암호화된 개인식별부호(CI)</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

certify\_win\_open("<?php echo $cert\_type; ?>", "<?php echo $cert\_url; ?>" + params);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\member\_confirm.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\member\_confirm.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fmemberconfirm" action="<?php echo $url ?>" onsubmit="return fmemberconfirm\_submit(this);" method="post">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\member\_confirm.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $member['mb\_id'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\member\_confirm.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="mb\_confirm\_id"><?php echo $member['mb\_id'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $g5['title'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="win\_total">전체 <?php echo $kind\_title ?>쪽지 <?php echo $total\_count ?>통<br></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php echo $readed; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($list[$i]['mb\_id']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['name']; ?> <span class="memo\_datetime"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$i]['send\_datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['view\_href'] ?>"><?php echo $memo\_preview; ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['del\_href'] ?>" onclick="del(this.href); return false;" class="memo\_del"><i class="fa fa-trash-o" aria-hidden="true"></i> <span class="sound\_only">삭제</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($i==0) { echo '<li class="empty\_table">자료가 없습니다.</li>'; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p class="win\_desc"><i class="fa fa-info-circle" aria-hidden="true"></i> 쪽지 보관일수는 최장 <strong><?php echo $config['cf\_memo\_del'] ?></strong>일 입니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fmemoform" action="<?php echo $memo\_action\_url; ?>" onsubmit="return fmemoform\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="me\_recv\_mb\_id" value="<?php echo $me\_recv\_mb\_id; ?>" id="me\_recv\_mb\_id" required class="frm\_input full\_input required" size="47" placeholder="받는 회원아이디">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($config['cf\_memo\_send\_point']) { ?><br>쪽지 보낼때 회원당 <?php echo number\_format($config['cf\_memo\_send\_point']); ?>점의 포인트를 차감합니다.<?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="me\_memo" id="me\_memo" required class="required"><?php echo $content ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($mb['mb\_id']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="memo\_view\_nick"><?php echo $nick ?></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="memo\_view\_date"><span class="sound\_only"><?php echo $kind\_date ?>시간</span><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $memo['me\_send\_datetime'] ?></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="memo\_op\_btn list\_btn"><a href="<?php echo $list\_link ?>" class="btn\_b01 btn"><i class="fa fa-list" aria-hidden="true"></i><span class="sound\_only">목록</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="memo\_op\_btn del\_btn"><a href="<?php echo $del\_link; ?>" onclick="del(this.href); return false;" class="memo\_del btn\_b01 btn"><i class="fa fa-trash-o" aria-hidden="true"></i> <span class="sound\_only">삭제</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $prev\_link ?>" class="btn\_left"><i class="fa fa-chevron-left" aria-hidden="true"></i> 이전쪽지</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $next\_link ?>" class="btn\_right">다음쪽지 <i class="fa fa-chevron-right" aria-hidden="true"></i></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($memo['me\_memo'], 0) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($kind == 'recv') { ?><a href="./memo\_form.php?me\_recv\_mb\_id=<?php echo $mb['mb\_id'] ?>&amp;me\_id=<?php echo $memo['me\_id'] ?>" class="reply\_btn">답장</a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fboardpassword" action="<?php echo $action; ?>" method="post">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comment\_id" value="<?php echo $comment\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\password\_lost.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fpasswordlost" action="<?php echo $action\_url ?>" onsubmit="return fpasswordlost\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\password\_lost.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

certify\_win\_open("<?php echo $cert\_type; ?>", "<?php echo $cert\_url; ?>"+params);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\password\_reset.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fpasswordreset" action="<?php echo $action\_url; ?>" onsubmit="return fpasswordreset\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\password\_reset.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_id" id="mb\_id" value="<?php echo $\_POST['mb\_id']; ?>" required class="required frm\_input full\_input" size="30" placeholder="아이디" readonly>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo number\_format($member['mb\_point']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php echo $point\_use\_class; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="point\_tit"><?php echo $po\_content; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="point\_num"><?php if ($point1) echo $point1; else echo $point2; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="point\_date1"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo conv\_date\_format('y-m-d H시', $row['po\_datetime']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="point\_date<?php echo $expr; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

만료 <?php echo substr(str\_replace('-', '', $row['po\_expire\_date']), 2); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php } else echo $row['po\_expire\_date'] == '9999-12-31' ? '&nbsp;' : $row['po\_expire\_date']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $sum\_point1; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $sum\_point2; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, $\_SERVER['SCRIPT\_NAME'].'?'.$qstr.'&amp;page='); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $mb\_nick ?>님의 프로필</h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $mb['mb\_level'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($mb['mb\_point']) ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><a href="<?php echo $mb\_homepage ?>" target="\_blank"><?php echo $mb\_homepage ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo ($member['mb\_level'] >= $mb['mb\_level']) ? substr($mb['mb\_datetime'],0,10) ." (".number\_format($mb\_reg\_after)." 일)" : "알 수 없음"; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo ($member['mb\_level'] >= $mb['mb\_level']) ? $mb['mb\_today\_login'] : "알 수 없음"; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo $mb\_profile ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fregister" id="fregister" action="<?php echo $register\_action\_url ?>" onsubmit="return fregister\_submit(this);" method="POST" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea readonly><?php echo get\_text($config['cf\_stipulation']) ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td>아이디, 이름, 비밀번호<?php echo ($config['cf\_cert\_use'])? ", 생년월일, 휴대폰 번호(본인인증 할 때만, 아이핀 제외), 암호화된 개인식별부호(CI)" : ""; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fregisterform" id="fregisterform" action="<?php echo $register\_action\_url ?>" onsubmit="return fregisterform\_submit(this);" method="post" enctype="multipart/form-data" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="agree" value="<?php echo $agree ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="agree2" value="<?php echo $agree2 ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cert\_type" value="<?php echo $member['mb\_certify']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (isset($member['mb\_sex'])) { ?><input type="hidden" name="mb\_sex" value="<?php echo $member['mb\_sex'] ?>"><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_nick\_default" value="<?php echo get\_text($member['mb\_nick']) ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_nick" value="<?php echo get\_text($member['mb\_nick']) ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_id" value="<?php echo $member['mb\_id'] ?>" id="reg\_mb\_id" class="frm\_input full\_input <?php echo $required ?> <?php echo $readonly ?>" minlength="3" maxlength="20" <?php echo $required ?> <?php echo $readonly ?> placeholder="아이디 (필수)">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="password" name="mb\_password" id="reg\_mb\_password" class="frm\_input full\_input <?php echo $required ?>" minlength="3" maxlength="20" <?php echo $required ?> placeholder="비밀번호 (필수)">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="password" name="mb\_password\_re" id="reg\_mb\_password\_re" class="frm\_input full\_input <?php echo $required ?>" minlength="3" maxlength="20" <?php echo $required ?> placeholder="비밀번호확인 (필수)">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $mb\_cert; ?> 본인확인</strong><?php if ($member['mb\_adult']) { ?> 및 <strong>성인인증</strong><?php } ?> 완료

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="reg\_mb\_name" class="sound\_only">이름 (필수)<?php echo $desc\_name ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" id="reg\_mb\_name" name="mb\_name" value="<?php echo get\_text($member['mb\_name']) ?>" <?php echo $required ?> <?php echo $name\_readonly; ?> class="frm\_input full\_input <?php echo $required ?> <?php echo $name\_readonly ?>" placeholder="이름 (필수)<?php echo $desc\_name ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

닉네임을 바꾸시면 앞으로 <?php echo (int)$config['cf\_nick\_modify'] ?>일 이내에는 변경 할 수 없습니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_nick\_default" value="<?php echo isset($member['mb\_nick'])?get\_text($member['mb\_nick']):''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_nick" value="<?php echo isset($member['mb\_nick'])?get\_text($member['mb\_nick']):''; ?>" id="reg\_mb\_nick" required class="frm\_input full\_input required nospace" maxlength="20" placeholder="닉네임 (필수)">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($w=='') { echo "E-mail 로 발송된 내용을 확인한 후 인증하셔야 회원가입이 완료됩니다."; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($w=='u') { echo "E-mail 주소를 변경하시면 다시 인증하셔야 합니다."; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="old\_email" value="<?php echo $member['mb\_email'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="email" name="mb\_email" value="<?php echo isset($member['mb\_email'])?$member['mb\_email']:''; ?>" id="reg\_mb\_email" required class="frm\_input email required" size="50" maxlength="100" placeholder="E-mail (필수)">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_homepage" value="<?php echo get\_text($member['mb\_homepage']) ?>" id="reg\_mb\_homepage" class="frm\_input full\_input <?php echo $config['cf\_req\_homepage']?"required":""; ?>" maxlength="255" <?php echo $config['cf\_req\_homepage']?"required":""; ?> placeholder="홈페이지<?php if ($config['cf\_req\_homepage']){ ?> (필수)<?php } ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_tel" value="<?php echo get\_text($member['mb\_tel']) ?>" id="reg\_mb\_tel" class="frm\_input full\_input <?php echo $config['cf\_req\_tel']?"required":""; ?>" maxlength="20" <?php echo $config['cf\_req\_tel']?"required":""; ?> placeholder="전화번호<?php if ($config['cf\_req\_tel']) { ?> (필수)<?php } ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="reg\_mb\_hp" class="sound\_only">휴대폰번호<?php if (!empty($hp\_required)) { ?> (필수)<?php } ?><?php echo $desc\_phone ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_hp" value="<?php echo get\_text($member['mb\_hp']) ?>" id="reg\_mb\_hp" <?php echo $hp\_required; ?> <?php echo $hp\_readonly; ?> class="frm\_input full\_input <?php echo $hp\_required; ?> <?php echo $hp\_readonly; ?>" maxlength="20" placeholder="휴대폰번호<?php if (!empty($hp\_required)) { ?> (필수)<?php } ?><?php echo $desc\_phone ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="old\_mb\_hp" value="<?php echo get\_text($member['mb\_hp']) ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="reg\_mb\_zip" class="sound\_only">우편번호<?php echo $config['cf\_req\_addr']?' (필수)':''; ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_zip" value="<?php echo $member['mb\_zip1'].$member['mb\_zip2']; ?>" id="reg\_mb\_zip" <?php echo $config['cf\_req\_addr']?"required":""; ?> class="frm\_input <?php echo $config['cf\_req\_addr']?"required":""; ?>" size="5" maxlength="6" placeholder="우편번호<?php echo $config['cf\_req\_addr']?' (필수)':''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="reg\_mb\_addr1" class="sound\_only">주소<?php echo $config['cf\_req\_addr']?' (필수)':''; ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_addr1" value="<?php echo get\_text($member['mb\_addr1']) ?>" id="reg\_mb\_addr1" <?php echo $config['cf\_req\_addr']?"required":""; ?> class="frm\_input frm\_address <?php echo $config['cf\_req\_addr']?"required":""; ?>" size="50" placeholder="주소<?php echo $config['cf\_req\_addr']?' (필수)':''; ?>"><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 156 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_addr2" value="<?php echo get\_text($member['mb\_addr2']) ?>" id="reg\_mb\_addr2" class="frm\_input frm\_address" size="50" placeholder="상세주소">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_addr3" value="<?php echo get\_text($member['mb\_addr3']) ?>" id="reg\_mb\_addr3" class="frm\_input frm\_address" size="50" readonly="readonly" placeholder="참고항목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 160 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_addr\_jibeon" value="<?php echo get\_text($member['mb\_addr\_jibeon']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="mb\_signature" id="reg\_mb\_signature" class="<?php echo $config['cf\_req\_signature']?"required":""; ?>" <?php echo $config['cf\_req\_signature']?"required":""; ?> placeholder="서명<?php if ($config['cf\_req\_signature']){ ?> (필수)<?php } ?>"><?php echo $member['mb\_signature'] ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="mb\_profile" id="reg\_mb\_profile" class="<?php echo $config['cf\_req\_profile']?"required":""; ?>" <?php echo $config['cf\_req\_profile']?"required":""; ?> placeholder="자기소개"><?php echo $member['mb\_profile'] ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 190 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

이미지 크기는 가로 <?php echo $config['cf\_member\_icon\_width'] ?>픽셀, 세로 <?php echo $config['cf\_member\_icon\_height'] ?>픽셀 이하로 해주세요.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 191 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

gif, jpg, png파일만 가능하며 용량 <?php echo number\_format($config['cf\_member\_icon\_size']) ?>바이트 이하만 등록됩니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 194 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<img src="<?php echo $mb\_icon\_url ?>" alt="회원아이콘">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 207 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

이미지 크기는 가로 <?php echo $config['cf\_member\_img\_width'] ?>픽셀, 세로 <?php echo $config['cf\_member\_img\_height'] ?>픽셀 이하로 해주세요.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 208 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

gif, jpg, png파일만 가능하며 용량 <?php echo number\_format($config['cf\_member\_img\_size']) ?>바이트 이하만 등록됩니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 211 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<img src="<?php echo $mb\_img\_url ?>" alt="회원아이콘">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 219 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="mb\_mailling" value="1" id="reg\_mb\_mailling" <?php echo ($w=='' || $member['mb\_mailling'])?'checked':''; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 229 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="mb\_sms" value="1" id="reg\_mb\_sms" <?php echo ($w=='' || $member['mb\_sms'])?'checked':''; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 240 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="mb\_open" value="1" id="reg\_mb\_open" <?php echo ($w=='' || $member['mb\_open'])?'checked':''; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 247 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

정보공개를 바꾸시면 앞으로 <?php echo (int)$config['cf\_open\_modify'] ?>일 이내에는 변경이 안됩니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 249 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_open\_default" value="<?php echo $member['mb\_open'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 254 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_open" value="<?php echo $member['mb\_open'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 257 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

정보공개는 수정후 <?php echo (int)$config['cf\_open\_modify'] ?>일 이내, <?php echo date("Y년 m월 j일", isset($member['mb\_open\_date']) ? strtotime("{$member['mb\_open\_date']} 00:00:00")+$config['cf\_open\_modify']\*86400:G5\_SERVER\_TIME+$config['cf\_open\_modify']\*86400); ?> 까지는 변경이 안됩니다.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 286 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="submit" id="btn\_submit" class="btn\_submit" accesskey="s"><?php echo $w==''?'회원가입':'정보수정'; ?></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 348 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

certify\_win\_open("<?php echo $cert\_type; ?>", "<?php echo $cert\_url; ?>"+params);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form\_update.tail.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$receive\_number = preg\_replace("/[^0-9]/", "", $mb\_hp);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_form\_update.tail.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace("/[^0-9]/", "", $default['de\_admin\_company\_tel']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo get\_text($mb['mb\_name']); ?></strong>님의 회원가입을 진심으로 축하합니다.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $mb['mb\_id'] ?></strong><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\register\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $mb['mb\_email'] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['opener\_href\_wr\_id'] ?>" target="\_blank" class="scrap\_tit" onclick="opener.document.location.href='<?php echo $list[$i]['opener\_href\_wr\_id'] ?>'; return false;"><?php echo $list[$i]['subject'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['opener\_href'] ?>" class="scrap\_cate" target="\_blank" onclick="opener.document.location.href='<?php echo $list[$i]['opener\_href'] ?>'; return false;"><?php echo $list[$i]['bo\_subject'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="scrap\_datetime"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$i]['ms\_datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['del\_href']; ?>" onclick="del(this.href); return false;" class="scrap\_del"><i class="fa fa-trash-o" aria-hidden="true"></i><span class="sound\_only">삭제</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($i == 0) echo "<li class=\"empty\_list\">자료가 없습니다.</li>"; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($config['cf\_mobile\_pages'], $page, $total\_page, "?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\scrap\_popin.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\scrap\_popin.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\member\basic\scrap\_popin.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_text(cut\_str($write['wr\_subject'], 255)) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $group\_select ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_id" value="<?php echo $mb\_id ?>" id="mb\_id" placeholder="검색어를 입력하세요" required class="frm\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.getElementById("gr\_id").value = "<?php echo $gr\_id ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.getElementById("view").value = "<?php echo $view ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($list[$i]['bo\_table']); ?>" class="new\_board"><?php echo $bo\_subject ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['href'] ?>" class="new\_tit"><?php echo $list[$i]['comment'] ?><?php echo $wr\_subject ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자</span><?php echo $list[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="new\_date"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$i]['datetime2'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($member['mb\_id']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $nick ?>님</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == 'super' || $is\_auth) { ?><a href="<?php echo G5\_ADMIN\_URL ?>" class="btn\_admin"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $memo\_not\_read ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $point ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($member['mb\_id'], 60, 60); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="nickname"><?php echo $nick ?>님</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_BBS\_URL ?>/point.php" target="\_blank" class="point win\_point"><strong><?php echo $point ?></strong> 포인트

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == 'super' || $is\_auth) { ?><a href="<?php echo G5\_ADMIN\_URL ?>" class="btn\_admin">관리자</a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $memo\_not\_read; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format(get\_shop\_member\_coupon\_count($member['mb\_id'], true)); ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="po\_id" value="<?php echo $po\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == "super") { ?><a href="<?php echo G5\_ADMIN\_URL ?>/poll\_form.php?w=u&amp;po\_id=<?php echo $po\_id ?>" class="btn\_admin btn"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자 관리</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo $po['po\_subject'] ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="gb\_poll" value="<?php echo $i ?>" id="gb\_poll\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="gb\_poll\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $po['po\_poll'.$i] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo " alert('권한 {$po['po\_level']} 이상의 회원만 투표에 참여하실 수 있습니다.'); return false; ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo " alert('권한 {$po['po\_level']} 이상의 회원만 결과를 보실 수 있습니다.'); return false; ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_all">전체 <?php echo $nf\_total\_po\_cnt ?>표</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $po\_subject ?> 결과</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php echo $poll\_1st\_class; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $list[$i]['content'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span style="width:<?php echo number\_format($list[$i]['rate'], 1) ?>%"></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="poll\_cnt"><?php echo $list[$i]['cnt'] ?> 표</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_percent"><?php echo number\_format($list[$i]['rate'], 1) ?> %</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $list2[$i]['pc\_name'] ?><span class="sound\_only">님의 의견</span></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list2[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_datetime"><?php echo $list2[$i]['datetime'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_cmt\_del"><?php if ($list2[$i]['del']) { echo $list2[$i]['del']."<i class=\"fa fa-times-circle\" aria-hidden=\"true\"></i><span class=\"sound\_only\">삭제</span></a>"; } ?></span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list2[$i]['idea'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="po\_id" value="<?php echo $po\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_member) { ?><input type="hidden" name="pc\_name" value="<?php echo get\_text(cut\_str($member['mb\_nick'],255)) ?>"><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h3><span>기타의견</span><?php echo $po\_etc ?></h3>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_guest) { echo chk\_captcha\_js(); } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo get\_text($token); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($admin\_href) { ?><li><a href="<?php echo $admin\_href ?>" class="btn\_admin btn"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="fix\_btn"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">문의등록</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $qaconfig['qa\_title'] ?> 카테고리</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="bo\_li<?php if ($is\_checkbox) echo ' bo\_adm'; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_qa\_id[]" value="<?php echo $list[$i]['qa\_id'] ?>" id="chk\_qa\_id\_<?php echo $i ?>" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_qa\_id\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<b class="sound\_only"><?php echo $list[$i]['subject'] ?></b>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="bo\_cate\_link"><?php echo $list[$i]['category']; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['view\_href']; ?>" class="bo\_subject">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['subject']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['icon\_file']) echo " <i class=\"fa fa-download\" aria-hidden=\"true\"></i>" ; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자</span><span><?php echo $list[$i]['name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_date"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$i]['date']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="li\_stat <?php echo ($list[$i]['qa\_status'] ? 'txt\_done' : 'txt\_rdy'); ?>"><?php echo ($list[$i]['qa\_status'] ? '답변완료' : '답변대기'); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($i == 0) { echo '<li class="empty\_list">게시물이 없습니다.</li>'; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list\_pages; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>전체 <?php echo number\_format($total\_count) ?>건</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $page ?> 페이지

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_qa\_sfl\_select\_options($sfl); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo stripslashes($stx) ?>" required placeholder="검색어를 입력하세요" id="stx" class="sch\_input" size="15" maxlength="15">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="tit\_cnt"><?php echo get\_text($answer['qa\_subject']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $answer['qa\_datetime']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_view\_thumbnail(conv\_content($answer['qa\_content'], $answer['qa\_html']), $qaconfig['qa\_image\_width']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $answer\_update\_href; ?>">답변수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $answer\_delete\_href; ?>" onclick="del(this.href); return false;">답변삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $rewrite\_href; ?>" class="add\_qu">추가질문</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qa\_id" value="<?php echo $view['qa\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo $token ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_hidden;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $option; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $list\_href ?>" class="btn\_b03 btn"><i class="fa fa-list" aria-hidden="true"></i><span class="sound\_only">목록</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $write\_href ?>" class="btn\_b03 btn"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($update\_href) { ?><li><a href="<?php echo $update\_href ?>"><i class="fa fa-pencil-square-o" aria-hidden="true"></i> 수정</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($delete\_href) { ?><li><a href="<?php echo $delete\_href ?>" onclick="del(this.href); return false;"><i class="fa fa-trash-o" aria-hidden="true"></i> 삭제</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_cate"><?php echo $view['category'] ;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_tit"><?php echo $view['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자</span><strong><?php echo $view['name'] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성일</span><strong><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $view['datetime']; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo $view['email']; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo $view['hp']; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_view\_thumbnail($view['img\_file'][$i], $qaconfig['qa\_image\_width']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="bo\_v\_con"><?php echo get\_view\_thumbnail($view['content'], $qaconfig['qa\_image\_width']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div><a href="<?php echo $rewrite\_href; ?>" class="btn\_b01">추가질문</a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['download\_href'][$i]; ?>" class="view\_file\_download" download>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<img src="<?php echo $qa\_skin\_url ?>/img/icon\_file.gif" alt="첨부">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $view['download\_source'][$i] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($prev\_href) { ?><li class="bo\_v\_prev"><a href="<?php echo $prev\_href ?>"><i class="fa fa-chevron-up" aria-hidden="true"></i><span class="sound\_only">이전글</span> <?php echo $prev\_qa\_subject;?></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($next\_href) { ?><li class="bo\_v\_next"><a href="<?php echo $next\_href ?>"><i class="fa fa-chevron-down" aria-hidden="true"></i><span class="sound\_only">다음글</span> <?php echo $next\_qa\_subject;?></a></li><?php } ?>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($qa\_skin\_path.'/view.answer.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($qa\_skin\_path.'/view.answerform.skin.php');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo get\_text($rel\_list[$i]['category']); ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $rel\_list[$i]['view\_href']; ?>" class="li\_sbj">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $rel\_list[$i]['subject']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="li\_stat <?php echo ($rel\_list[$i]['qa\_status'] ? 'txt\_done' : 'txt\_rdy'); ?>"><?php echo ($rel\_list[$i]['qa\_status'] ? '답변완료' : '답변대기'); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="li\_date"><?php echo $rel\_list[$i]['date']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fwrite" id="fwrite" action="<?php echo $action\_url ?>" onsubmit="return fwrite\_submit(this);" method="post" enctype="multipart/form-data" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qa\_id" value="<?php echo $qa\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo $token ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_hidden;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $option; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="email" name="qa\_email" value="<?php echo get\_text($write['qa\_email']); ?>" id="qa\_email" <?php echo $req\_email; ?> class="<?php echo $req\_email.' '; ?>frm\_input full\_input email" maxlength="100" placeholder="이메일">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qa\_email\_recv" value="1" id="qa\_email\_recv" <?php if($write['qa\_email\_recv']) echo 'checked="checked"'; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_hp" value="<?php echo get\_text($write['qa\_hp']); ?>" id="qa\_hp" <?php echo $req\_hp; ?> class="<?php echo $req\_hp.' '; ?>frm\_input full\_input" size="30" placeholder="휴대폰">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qa\_sms\_recv" value="1" id="qa\_sms\_recv" <?php if($write['qa\_sms\_recv']) echo 'checked="checked"'; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_subject" value="<?php echo get\_text($write['qa\_subject']); ?>" id="qa\_subject" required class="frm\_input full\_input required" maxlength="255" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="file" name="bf\_file[1]" id="bf\_file[1]" title="파일첨부 1 : 용량 <?php echo $upload\_max\_filesize; ?> 이하만 업로드 가능" class="frm\_file uploadBtn">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bf\_file\_del1"><?php echo $write['qa\_source1']; ?> 파일 삭제</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="file" name="bf\_file[2]" id="bf\_file[2]" title="파일첨부 2 : 용량 <?php echo $upload\_max\_filesize; ?> 이하만 업로드 가능" class="frm\_file uploadBtn">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bf\_file\_del2"><?php echo $write['qa\_source2']; ?> 파일 삭제</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list\_href; ?>" class="btn\_cancel">취소</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li>게시판<strong><?php echo $board\_count ?>개</strong></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li>게시물<strong><?php echo number\_format($total\_count) ?>개</strong></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><?php echo number\_format($page) ?>/<?php echo number\_format($total\_page) ?> 페이지 열람 중</li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="srows" value="<?php echo $srows ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $group\_select ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<script>document.getElementById("gr\_id").value = "<?php echo $gr\_id ?>";</script>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="wr\_subject||wr\_content"<?php echo get\_selected($sfl, "wr\_subject||wr\_content") ?>>제목+내용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="wr\_subject"<?php echo get\_selected($sfl, "wr\_subject") ?>>제목</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="wr\_content"<?php echo get\_selected($sfl, "wr\_content") ?>>내용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mb\_id"<?php echo get\_selected($sfl, "mb\_id") ?>>회원아이디</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="wr\_name"<?php echo get\_selected($sfl, "wr\_name") ?>>이름</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" id="stx" value="<?php echo $text\_stx ?>" class="frm\_input" required maxlength="20">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" value="or" <?php echo ($sop == "or") ? "checked" : ""; ?> id="sop\_or" name="sop">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" value="and" <?php echo ($sop == "and") ? "checked" : ""; ?> id="sop\_and" name="sop">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="?<?php echo $search\_query ?>&amp;gr\_id=<?php echo $gr\_id ?>" <?php echo $sch\_all ?>>전체게시판</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str\_board\_list; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><a href="<?php echo get\_pretty\_url($search\_table[$idx], '', $search\_query); ?>"><?php echo $bo\_subject[$idx] ?> 게시판 내 결과</a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$idx][$i]['href'] ?><?php echo $comment\_href ?>"><?php echo $comment\_def ?><?php echo $list[$idx][$i]['subject'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <a href="<?php echo $list[$idx][$i]['href'] ?><?php echo $comment\_href ?>" target="\_blank" class="sch\_res\_new"><i class="fa fa-share-square-o" aria-hidden="true"></i><span class="sound\_only">새창</span></a> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo $list[$idx][$i]['content'] ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$idx][$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sch\_datetime"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$idx][$i]['wr\_datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sch\_more"><a href="<?php echo get\_pretty\_url($search\_table[$idx], '', $search\_query); ?>"><strong><?php echo $bo\_subject[$idx] ?></strong> 결과 더보기</a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\boxbanner.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i==0) echo '<aside id="sbn\_side"><h2>쇼핑몰 배너</h2><ul class="sb\_bn">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\boxbanner.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $banner.'<img src="'.G5\_DATA\_URL.'/banner/'.$row['bn\_id'].'" alt="'.get\_text($row['bn\_alt']).'" width="'.$size[0].'" height="'.$size[1].'"'.$bn\_border.'>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\boxbanner.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i>0) echo '</ul></aside>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($tv\_tot\_count == 0) echo '<ul id="stv\_ul">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li class="stv\_item c'.$k.'">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $img;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($tv\_tot\_count > 0) echo '</ul>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var itemQty = <?php echo $tv\_tot\_count; ?>;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var itemShow = <?php echo $tv\_div['img\_length']; ?>;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var EOFlag = parseInt(<?php echo $i-1; ?>/itemShow);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var itemRest = parseInt(<?php echo $i-1; ?>%itemShow);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\couponzone.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo $default['de\_admin\_company\_name']; ?> 회원이시라면 쿠폰 다운로드 후 바로 사용하실 수 있습니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\couponzone.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<ul>'.PHP\_EOL.$coupon.'</ul>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\couponzone.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p>보유하신 <?php echo $default['de\_admin\_company\_name']; ?> 회원 포인트를 쿠폰으로 교환하실 수 있습니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 181 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\couponzone.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<ul>'.PHP\_EOL.$coupon.'</ul>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

Kakao.init("<?php echo $config['cf\_kakao\_js\_apikey']; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fitem" action="<?php echo $action\_url; ?>" method="post" onsubmit="return fitem\_submit(this);">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[]" value="<?php echo $it['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $thumb\_img;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong id="sit\_title"><?php echo stripslashes($it['it\_name']); ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($it['it\_basic']) { ?><p id="sit\_desc"><?php echo $it['it\_basic']; ?></p><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p id="sit\_opt\_info">상품 선택옵션 <?php echo $option\_count; ?> 개, 추가옵션 <?php echo $supply\_count; ?> 개</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">고객평점 <?php echo $score?>개</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<img src="<?php echo G5\_SHOP\_URL; ?>/img/s\_star<?php echo $score?>.png" alt="" class="sit\_star" width="100">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="review\_num">사용후기 <?php echo $it['it\_use\_cnt']; ?> 개</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="btn\_wish"><i class="fa fa-heart-o" aria-hidden="true"></i><span class="sound\_only">위시리스트</span><span class="btn\_wish\_num"><?php echo get\_wishlist\_count\_by\_item($it['it\_id']); ?></span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/facebook.png'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/twitter.png'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/gplus.png'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_sns\_share\_link('kakaotalk', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/sns\_kakao.png'); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:popup\_item\_recommend('<?php echo $it['it\_id']; ?>');" id="sit\_btn\_rec"><i class="fa fa-envelope-o" aria-hidden="true"></i><span class="sound\_only">추천하기</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $it['it\_maker']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $it['it\_origin']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $it['it\_brand']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $it['it\_model']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_price($it['it\_cust\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo display\_price(get\_price($it)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="it\_price" value="<?php echo get\_price($it); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 174 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '구매금액(추가옵션 제외)의 '.$it['it\_point'].'%';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo number\_format($it\_point).'점';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 203 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th><?php echo $ct\_send\_cost\_label; ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 204 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $sc\_method; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 209 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($it['it\_buy\_min\_qty']); ?> 개</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 215 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($it['it\_buy\_max\_qty']); ?> 개</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 230 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $prev\_href.$prev\_title.$prev\_href2;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 231 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $next\_href.$next\_title.$next\_href2;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_SHOP\_URL; ?>/largeimage.php?it\_id=<?php echo $it['it\_id']; ?>&amp;no=1" target="\_blank" class="popup\_item\_image "><i class="fa fa-search-plus" aria-hidden="true"></i><span class="sound\_only">확대보기</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 255 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_item;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 271 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $supply\_item;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 288 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_type[<?php echo $it\_id; ?>][]" value="0">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 289 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_id[<?php echo $it\_id; ?>][]" value="">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 290 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_value[<?php echo $it\_id; ?>][]" value="<?php echo $it['it\_name']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 292 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" class="io\_stock" value="<?php echo $it['it\_stock\_qty']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 294 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sit\_opt\_subj"><?php echo $it['it\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 297 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ct\_qty\_<?php echo $i; ?>" class="sound\_only">수량</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 299 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ct\_qty[<?php echo $it\_id; ?>][]" value="<?php echo $it['it\_buy\_min\_qty']; ?>" id="ct\_qty\_<?php echo $i; ?>" class="num\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 325 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:popup\_stocksms('<?php echo $it['it\_id']; ?>');" id="sit\_btn\_phone">재입고알림</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 327 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:item\_wish(document.fitem, '<?php echo $it['it\_id']; ?>');" id="sit\_btn\_wish"><span class="sound\_only">위시리스트</span><i class="fa fa-heart-o" aria-hidden="true"></i></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 329 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="naverpay-item"><?php echo $naverpay\_request\_js.$naverpay\_button\_js; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 363 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo ($it['it\_mobile\_explan'] ? conv\_content($it['it\_mobile\_explan'], 1) : conv\_content($it['it\_explan'], 1)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 383 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><?php echo $ii\_title; ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 384 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $ii\_value; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 421 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($default['de\_baesong\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 431 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($default['de\_change\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 465 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 573 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var min\_qty = parseInt(<?php echo $it['it\_buy\_min\_qty']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 574 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var max\_qty = parseInt(<?php echo $it['it\_buy\_max\_qty']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 623 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

f.action = "<?php echo $action\_url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 645 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var min\_qty = parseInt(<?php echo $it['it\_buy\_min\_qty']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 646 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var max\_qty = parseInt(<?php echo $it['it\_buy\_max\_qty']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\iteminfo.change.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($default['de\_change\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\iteminfo.delivery.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($default['de\_baesong\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\iteminfo.delivery.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($default['de\_change\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\iteminfo.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $it['it\_basic']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\iteminfo.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo ($it['it\_mobile\_explan'] ? conv\_content($it['it\_mobile\_explan'], 1) : conv\_content($it['it\_explan'], 1)); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\iteminfo.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $ii\_title; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\iteminfo.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $ii\_value; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\iteminfo.relation.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemqa\_form; ?>" class="itemqa\_form qa\_wr">상품문의 쓰기<span class="sound\_only"> 새 창</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemqa\_list; ?>" id="itemqa\_list" class="btn01">더보기</a>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqa.skin.php

MD5 Hashing algorithm.

$hash = md5($row['iq\_id'].$row['iq\_time'].$row['iq\_ip']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<ol id="sit\_qa\_ol">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" class="sit\_qa\_li\_title"><?php echo $iq\_subject; ?></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo $iq\_name; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $iq\_time; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="<?php echo $iq\_style; ?>"><?php echo $iq\_stats; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sit\_qa\_con\_<?php echo $i; ?>" class="sit\_qa\_con">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $iq\_question;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $iq\_answer; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemqa\_form."&amp;iq\_id={$row['iq\_id']}&amp;w=u"; ?>" class="itemqa\_form btn01" onclick="return false;">수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemqa\_formupdate."&amp;iq\_id={$row['iq\_id']}&amp;w=d&amp;hash={$hash}"; ?>" class="itemqa\_delete btn01">삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo '</ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (!$i) echo '<p class="sit\_empty">상품문의가 없습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo itemqa\_page($config['cf\_mobile\_pages'], $page, $total\_page, G5\_SHOP\_URL."/itemqa.php?it\_id=$it\_id&amp;page=", "");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id" value="<?php echo $it\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="iq\_id" value="<?php echo $iq\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="iq\_secret" id="iq\_secret" value="1" <?php echo $chk\_secret; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="email" name="iq\_email" id="iq\_email" value="<?php echo get\_text($qa['iq\_email']); ?>" class="frm\_input full\_input" size="30" placeholder="이메일"> <span class="frm\_info ">이메일을 입력하시면 답변 등록 시 답변이 이메일로 전송됩니다.</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="iq\_hp" id="iq\_hp" value="<?php echo get\_text($qa['iq\_hp']); ?>" class="frm\_input full\_input" size="20" placeholder="휴대폰"> <span class="frm\_info ">휴대폰번호를 입력하시면 답변 등록 시 답변등록 알림이 SMS로 전송됩니다.</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="iq\_subject" value="<?php echo get\_text($qa['iq\_subject']); ?>" id="iq\_subject" required class="required frm\_input full\_input" minlength="2" maxlength="250" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form method="get" action="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="b.it\_name" <?php echo get\_selected($sfl, "b.it\_name", true); ?>>상품명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.it\_id" <?php echo get\_selected($sfl, "a.it\_id"); ?>>상품코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.iq\_subject" <?php echo get\_selected($sfl, "a.iq\_subject"); ?>>문의제목</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.iq\_question"<?php echo get\_selected($sfl, "a.iq\_question"); ?>>문의내용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.iq\_name" <?php echo get\_selected($sfl, "a.it\_id"); ?>>작성자명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.mb\_id" <?php echo get\_selected($sfl, "a.mb\_id"); ?>>작성자아이디</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx; ?>" id="stx" required class="sch\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">전체보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <p><?php echo $config['cf\_title']; ?> 전체 상품문의 목록입니다.</p> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $it\_href; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_it\_image($row['it\_id'], 60, 60); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $row['it\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><span class="<?php echo $iq\_style; ?>"><?php echo $iq\_stats; ?></span> <?php echo $iq\_subject; ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sqa\_if\_wt"><?php echo get\_text($row['iq\_name']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo substr($row['iq\_time'],2,8); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sqa\_con\_<?php echo $i; ?>" class="sqa\_con" style="display:none;">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $iq\_question;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $iq\_answer; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sqa\_con\_btn"><button class="sqa\_con\_<?php echo $i; ?>"><span class="sound\_only">내용보기</span><i class="fa fa-chevron-down" aria-hidden="true"></i></button></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo '</ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<p id="sps\_empty">자료가 없습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($config['cf\_mobile\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemuse\_form; ?>" class="qa\_wr itemuse\_form " onclick="return false;">사용후기 쓰기<span class="sound\_only"> 새 창</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemuse\_list; ?>" id="itemuse\_list" class="btn01">더보기</a>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuse.skin.php

MD5 Hashing algorithm.

$hash = md5($row['is\_id'].$row['is\_time'].$row['is\_ip']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<ol id="sit\_use\_ol">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" class="sit\_use\_li\_title"><?php echo $is\_subject; ?></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo $is\_name; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $is\_time; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sit\_use\_star"><img src="<?php echo G5\_SHOP\_URL; ?>/img/s\_star<?php echo $is\_star; ?>.png" alt="별<?php echo $is\_star; ?>개"></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sit\_use\_con\_<?php echo $i; ?>" class="sit\_use\_con">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemuse\_form."&amp;is\_id={$row['is\_id']}&amp;w=u"; ?>" class="itemuse\_form btn01" onclick="return false;">수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemuse\_formupdate."&amp;is\_id={$row['is\_id']}&amp;w=d&amp;hash={$hash}"; ?>" class="itemuse\_delete btn01">삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_reply\_subject;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_reply\_name;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_reply\_content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo '</ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (!$i) echo '<p class="sit\_empty">사용후기가 없습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo itemuse\_page($config['cf\_mobile\_pages'], $page, $total\_page, G5\_SHOP\_URL."/itemuse.php?it\_id=$it\_id&amp;page=", "");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id" value="<?php echo $it\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="is\_id" value="<?php echo $is\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="is\_subject" value="<?php echo get\_text($use['is\_subject']); ?>" id="is\_subject" required class="required frm\_input" minlength="2" maxlength="250" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="5" id="is\_score10" <?php echo ($is\_score==5)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="4" id="is\_score8" <?php echo ($is\_score==4)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="3" id="is\_score6" <?php echo ($is\_score==3)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="2" id="is\_score4" <?php echo ($is\_score==2)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="1" id="is\_score2" <?php echo ($is\_score==1)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form method="get" action="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="b.it\_name" <?php echo get\_selected($sfl, "b.it\_name"); ?>>상품명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.it\_id" <?php echo get\_selected($sfl, "a.it\_id"); ?>>상품코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.is\_subject"<?php echo get\_selected($sfl, "a.is\_subject"); ?>>후기제목</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.is\_content"<?php echo get\_selected($sfl, "a.is\_content"); ?>>후기내용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.is\_name" <?php echo get\_selected($sfl, "a.is\_name"); ?>>작성자명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.mb\_id" <?php echo get\_selected($sfl, "a.mb\_id"); ?>>작성자아이디</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx; ?>" id="stx" required class="sch\_input" size="10">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">전체보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <p><?php echo $config['cf\_title']; ?> 전체 사용후기 목록입니다.</p> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $it\_href; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_itemuselist\_thumbnail($row['it\_id'], $row['is\_content'], 70, 70); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $row2['it\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">평가점수</span><img src="<?php echo G5\_SHOP\_URL; ?>/img/s\_star<?php echo $star; ?>.png" alt="별<?php echo $star; ?>개" width="80">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button class="sps\_con\_<?php echo $i; ?> review\_detail"><?php echo get\_text($row['is\_subject']); ?></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo get\_text($row['is\_subject']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sps\_dd\_wt"><?php echo $row['is\_name']; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo substr($row['is\_time'],0,10); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_itemuselist\_thumbnail($row['it\_id'], $row['is\_content'], 50, 50); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo get\_text($row['is\_subject']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">평가점수</span><img src="<?php echo G5\_URL; ?>/shop/img/s\_star<?php echo $star; ?>.png" alt="별<?php echo $star; ?>개" width="80">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sps\_con\_<?php echo $i; ?>" class="review\_bt\_cnt">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="is\_use\_reply"><?php echo get\_text($row['is\_reply\_subject']); ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $row['is\_reply\_name']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sps\_con\_<?php echo $i; ?>\_reply">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_reply\_content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sps\_if\_wt"><?php echo get\_text($row['is\_name']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo substr($row['is\_time'],2,8); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo '</ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<p id="sps\_empty">자료가 없습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($config['cf\_mobile\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\largeimage.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<img src="<?php echo $imageurl; ?>" width="<?php echo $size[0]; ?>" alt="<?php echo $row['it\_name']; ?>" id="largeimage\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\largeimage.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><a href="'.G5\_SHOP\_URL.'/largeimage.php?it\_id='.$it\_id.'&amp;no='.$key.'" class="img\_thumb">'.$val.'</a></li>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\largeimage.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$("#sit\_pvi\_nwbig span:eq("+<?php echo ($no - 1); ?>+")").addClass("visible");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

Kakao.init("<?php echo $config['cf\_kakao\_js\_apikey']; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul id=\"sct\_wrap\" class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul id=\"sct\_wrap\" class=\"sct ".$ul\_sct\_class."\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$li\_clear}\"$li\_width\_style><div class=\"li\_wr is\_view\_type\_list\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_star\"><span class=\"sound\_only\">고객평점</span><img src=\"".G5\_SHOP\_URL."/img/s\_star".$star\_score.".png\" alt=\"별점 ".$star\_score."점\" class=\"sit\_star\"></div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_basic\">".stripslashes($row['it\_basic'])."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<button type=\"button\" class=\"btn\_wish\" data-it\_id=\"{$row['it\_id']}\"><span class=\"sound\_only\">위시리스트</span><i class=\"fa fa-heart-o\" aria-hidden=\"true\"></i></button>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/facebook.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/twitter.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/gplus.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('kakaotalk', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/sns\_kakao.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_icon\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var li\_width = "<?php echo intval(100 / $this->list\_mod); ?>",

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

img\_width = "<?php echo $this->img\_width; ?>",

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 151 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

img\_height = "<?php echo $this->img\_height; ?>",

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

list\_ca\_id = "<?php echo $this->ca\_id; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.best.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li class="sct\_li"'.$li\_width\_style.'>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.best.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="sct\_img"><a href="'.$this->href.$row['it\_id'].'" class="sct\_a">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.best.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name'])).PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.best.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="sct\_id">&lt;'.stripslashes($row['it\_id']).'&gt;</div>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.best.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="sct\_txt"><a href="'.$this->href.$row['it\_id'].'" class="sct\_a">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.best.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name']).PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.best.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="sct\_cost">'.display\_price(get\_price($row), $row['it\_tel\_inq']).'</div>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.best.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="bst\_silde\_btn">'.$slide\_btn.'</div>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_price&amp;sortodr=asc" >낮은가격순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_price&amp;sortodr=desc">높은가격순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_name&amp;sortodr=asc">상품명순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\listcategory.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

Kakao.init("<?php echo $config['cf\_kakao\_js\_apikey']; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$li\_clear}\"$li\_width\_style><div class=\"li\_wr is\_view\_type\_list\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_star\"><img src=\"".G5\_SHOP\_URL."/img/s\_star".$star\_score.".png\" alt=\"별점 ".$star\_score."점\" class=\"sit\_star\"></div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$this->href}{$row['it\_id']}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_basic\">".stripslashes($row['it\_basic'])."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<button type=\"button\" class=\"btn\_wish\" data-it\_id=\"{$row['it\_id']}\"><span class=\"sound\_only\">위시리스트</span><i class=\"fa fa-heart-o\" aria-hidden=\"true\"></i></button>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/facebook.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/twitter.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/gplus.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('kakaotalk', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/sns\_kakao.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_icon\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

Kakao.init("<?php echo $config['cf\_kakao\_js\_apikey']; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$li\_clear}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"li\_wr\" style=\"padding-left:{$this->img\_width}px;height:{$this->img\_height}px\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_star\"><img src=\"".G5\_SHOP\_URL."/img/s\_star".$star\_score.".png\" alt=\"별점 ".$star\_score."점\" class=\"sit\_star\"></div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$this->href}{$row['it\_id']}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_icon\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_sns\" style=\"top:{$sns\_top}px\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/facebook.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/twitter.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/gplus.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('kakaotalk', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/sns\_kakao.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

Kakao.init("<?php echo $config['cf\_kakao\_js\_apikey']; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$li\_clear}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_star\"><img src=\"".G5\_SHOP\_URL."/img/s\_star".$star\_score.".png\" alt=\"별점 ".$star\_score."점\" class=\"sit\_star\"></div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$this->href}{$row['it\_id']}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_sns\" style=\"top:{$sns\_top}px\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/facebook.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/twitter.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/gplus.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('kakaotalk', $sns\_url, $sns\_title, G5\_MSHOP\_SKIN\_URL.'/img/sns\_kakao.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.event.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="'.$href.'" class="sev\_img"><img src="'.G5\_DATA\_URL.'/event/'.$row['ev\_id'].'\_m" alt="'.$row['ev\_subject'].'"></a>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.event.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="'.$href.'" class="sev\_text">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.event.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($row['ev\_subject\_strong']) echo '<strong>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.event.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $row['ev\_subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.event.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($row['ev\_subject\_strong']) echo '</strong>';

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.event.skin.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

from `{$g5['g5\_shop\_event\_item\_table']}` a left join `{$g5['g5\_shop\_item\_table']}` b on (a.it\_id = b.it\_id)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.event.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li class="ev\_prd\_'.$k.'">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\main.event.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<span class="ev\_prd\_img">'.get\_it\_image($row2['it\_id'], 300, 300, get\_text($row2['it\_name'])).'</span>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\mainbanner.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i==0) echo '<div id="main\_bn"><div class="main\_banner\_owl owl-carousel">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\mainbanner.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $banner.'<img src="'.G5\_DATA\_URL.'/banner/'.$row['bn\_id'].'" width="'.$size[0].'" alt="'.get\_text($row['bn\_alt']).'"'.$bn\_border.'>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\navigation.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="sct\_li<?php echo $li\_clear; ?>"<?php echo $li\_width\_style; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sct\_img"><a href="<?php echo $href; ?>" class="sct\_a"><img src="<?php echo G5\_MSHOP\_SKIN\_URL; ?>/img/personal.jpg" alt=""></a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sct\_txt"><a href="<?php echo $href; ?>" class="sct\_a"><?php echo get\_text($row['pp\_name']).'님 개인결제'; ?></a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sct\_cost"><?php echo display\_price($row['pp\_price']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 개인결제가 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

Kakao.init("<?php echo $config['cf\_kakao\_js\_apikey']; ?>");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul id=\"sct\_wrap\" class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$li\_clear}\"$li\_width\_style><div class=\"li\_wr\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"{$item\_link\_href}\" class=\"sct\_txt\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 관련상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

검색 결과 <b><?php echo $total\_count; ?></b>건

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qsort" id="qsort" value="<?php echo $qsort ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qorder" id="qorder" value="<?php echo $qorder ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qcaid" id="qcaid" value="<?php echo $qcaid ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="q" value="<?php echo $q; ?>" id="ssch\_q" class="frm\_input" maxlength="30">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qname" id="ssch\_qname" <?php echo $qname\_check?'checked="checked"':'';?> class="selec\_chk"> <label for="ssch\_qname"><span></span>상품명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qexplan" id="ssch\_qexplan" <?php echo $qexplan\_check?'checked="checked"':'';?> class="selec\_chk"> <label for="ssch\_qexplan"><span></span> <span class="sound\_only">상품</span>설명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qbasic" id="ssch\_qbasic" value="1" <?php echo $qbasic\_check?'checked="checked"':'';?> class="selec\_chk"> <label for="ssch\_qbasic"><span></span> 기본설명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qid" id="ssch\_qid" <?php echo $qid\_check?'checked="checked"':'';?> class="selec\_chk"> <label for="ssch\_qid"><span></span><span class="sound\_only"> 상품</span>코드</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qfrom" value="<?php echo $qfrom; ?>" id="ssch\_qfrom" class="frm\_input" size="6"> 원 ~

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qto" value="<?php echo $qto; ?>" id="ssch\_qto" class="frm\_input" size="6"> 원<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><a href="#" onclick="set\_ca\_id(\'\'); return false;">전체분류 <span>'.$total\_count.'</span></a></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li><a href=\"#\" onclick=\"set\_ca\_id('{$row['ca\_id']}'); return false;\">{$row['ca\_name']} <span>".$row['cnt']."</span></a></li>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div>'.$error.'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_paging($config['cf\_mobile\_pages'], $page, $total\_page, $\_SERVER['SCRIPT\_NAME'].'?'.$query\_string.'&amp;page=');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo number\_format($visit[1]) ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo number\_format($visit[2]) ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo number\_format($visit[3]) ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo number\_format($visit[4]) ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\mobile\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == "super") { ?><a href="<?php echo G5\_ADMIN\_URL ?>/visit\_list.php" class="btn\_admin btn"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">상세보기</span></a></a><?php } ?>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 4 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\ajax.action.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$action = isset($\_REQUEST['action']) ? preg\_replace('/[^a-z0-9\_]/i', '', $\_REQUEST['action']) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\ajax.action.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$s\_cart\_id = preg\_replace('/[^a-z0-9\_\-]/i', '', get\_session('ss\_cart\_id'));

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\ajax.action.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$tmp\_cart\_id = preg\_replace('/[^a-z0-9\_\-]/i', '', $tmp\_cart\_id);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\ajax.action.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$io\_id = isset($\_POST['io\_id'][$it\_id][$k]) ? preg\_replace(G5\_OPTION\_ID\_FILTER, '', $\_POST['io\_id'][$it\_id][$k]) : '';

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\ajax.action.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$io\_type = isset($\_POST['io\_type'][$it\_id][$k]) ? preg\_replace('#[^01]#', '', $\_POST['io\_type'][$it\_id][$k]) : '';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 278 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fcart" method="post" action="<?php echo $action\_url; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 280 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[]" value="<?php echo $it['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 281 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_name[]" value="<?php echo stripslashes($it['it\_name']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 282 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_price[]" value="<?php echo get\_price($it); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 283 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_stock[]" value="<?php echo get\_it\_stock\_qty($it['it\_id']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 284 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_type[<?php echo $it['it\_id']; ?>][]" value="0">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 285 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_id[<?php echo $it['it\_id']; ?>][]" value="">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 286 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_value[<?php echo $it['it\_id']; ?>][]" value="">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 287 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_price[<?php echo $it['it\_id']; ?>][]" value="">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 288 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ct\_qty[<?php echo $it['it\_id']; ?>][]" value="<?php echo $item\_ct\_qty; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 296 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\ajax.action.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_item;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $mshop\_ca\_row1['url']; ?>" class="cate\_li\_1\_a"><?php echo get\_text($mshop\_ca\_row1['ca\_name']); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\category.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $mshop\_ca\_row2['url']; ?>"><?php echo get\_text($mshop\_ca\_row2['ca\_name']); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\index.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="my\_ov\_name"><?php echo get\_member\_profile\_img($member['mb\_id']); ?><br><?php echo $member['mb\_name']; ?></strong><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($member['mb\_point']); ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($cp\_count); ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $memo\_not\_read ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="scrap"><?php echo number\_format($member['mb\_scrap\_cnt']); ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo ($member['mb\_tel'] ? $member['mb\_tel'] : '미등록'); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo ($member['mb\_email'] ? $member['mb\_email'] : '미등록'); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo $member['mb\_today\_login']; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo $member['mb\_datetime']; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd id="smb\_my\_ovaddd"><?php echo sprintf("(%s%s)", $member['mb\_zip1'], $member['mb\_zip2']).' '.print\_address($member['mb\_addr1'], $member['mb\_addr2'], $member['mb\_addr3'], $member['mb\_addr\_jibeon']); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_it\_id[<?php echo $i; ?>]" value="1" id="chk\_it\_id\_<?php echo $i; ?>" onclick="out\_cd\_check(this, '<?php echo $out\_cd; ?>');" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_it\_id\_<?php echo $i; ?>"><span></span><b class="sound\_only"><?php echo $row['it\_name']; ?></b></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[<?php echo $i; ?>]" value="<?php echo $row['it\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_type[<?php echo $row['it\_id']; ?>][0]" value="0">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_id[<?php echo $row['it\_id']; ?>][0]" value="">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_value[<?php echo $row['it\_id']; ?>][0]" value="<?php echo $row['it\_name']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 137 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="ct\_qty[<?php echo $row['it\_id']; ?>][0]" value="1">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="smb\_my\_img"><?php echo $image; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="smb\_my\_tit"><a href="<?php echo shop\_item\_url($row['it\_id']); ?>"><?php echo stripslashes($row['it\_name']); ?></a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="smb\_my\_price"><?php echo display\_price(get\_price($row), $row['it\_tel\_inq']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="smb\_my\_date"><?php echo $row['wi\_time']; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\mypage.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="./wishupdate.php?w=d&amp;wi\_id=<?php echo $row['wi\_id']; ?>" class="wish\_del"><i class="fa fa-trash" aria-hidden="true"></i><span class="sound\_only">삭제</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sod\_fin\_no">주문번호 <strong><?php echo $od\_id; ?></strong></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sod\_img"><?php echo $image; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo shop\_item\_url($row['it\_id']); ?>"><?php echo $row['it\_name']; ?></a><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sod\_opt"><?php echo get\_text($opt['ct\_option']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_itqty" class="td\_mngsmall"><?php echo number\_format($opt['ct\_qty']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_itprice" class="td\_numbig text\_right"><?php echo number\_format($opt\_price); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_itpt" class="td\_numbig text\_right"><?php echo number\_format($point); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_itsd" class="td\_dvr"><?php echo $ct\_send\_cost; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_itsum" class="td\_numbig text\_right"><?php echo number\_format($sell\_price); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td headers="th\_itst" class="td\_mngsmall"><?php echo $opt['ct\_status']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 221 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 225 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_tel']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 229 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_hp']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 233 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text(sprintf("(%s%s)", $od['od\_zip1'], $od['od\_zip2']).' '.print\_address($od['od\_addr1'], $od['od\_addr2'], $od['od\_addr3'], $od['od\_addr\_jibeon'])); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 237 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_email']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 253 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_b\_name']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 257 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_b\_tel']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 261 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text($od['od\_b\_hp']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 265 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo get\_text(sprintf("(%s%s)", $od['od\_b\_zip1'], $od['od\_b\_zip2']).' '.print\_address($od['od\_b\_addr1'], $od['od\_b\_addr2'], $od['od\_b\_addr3'], $od['od\_b\_addr\_jibeon'])); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 274 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo substr($od['od\_hope\_date'],0,10).' ('.get\_yoil($od['od\_hope\_date']).')' ;?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 282 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo conv\_content($od['od\_memo'], 0); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 299 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od['od\_delivery\_company']; ?> <?php echo get\_delivery\_inquiry($od['od\_delivery\_company'], $od['od\_invoice'], 'dvr\_link'); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 303 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od['od\_invoice']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 307 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $od['od\_invoice\_time']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 324 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($od['od\_cart\_price']); ?> 원</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 329 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($od['od\_cart\_coupon']); ?> 원</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 335 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($od['od\_coupon']); ?> 원</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 341 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($od['od\_send\_cost']); ?> 원</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 347 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($od['od\_send\_coupon']); ?> 원</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 353 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($od['od\_send\_cost2']); ?> 원</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 359 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($od['od\_cancel\_price']); ?> 원</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 364 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($tot\_price); ?> 원</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 368 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($tot\_point); ?> 점</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 371 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="sod\_fin\_tot"><span>총 구매액</span><strong><?php echo display\_price($tot\_price); ?></strong></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 376 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<strong>'.display\_price($misu\_price).'</strong>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 382 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $wanbul; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 385 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><span class="title">포인트 결제</span><?php echo number\_format($od['od\_receipt\_point']); ?>점</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 386 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><span class="title">실결제</span><?php echo number\_format($od['od\_receipt\_price']); ?>원</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 397 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $od\_id; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 401 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $od['od\_time']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 405 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo check\_pay\_name\_replace($od['od\_settle\_case'], $od, 1); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 409 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $od\_receipt\_price; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 417 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $od['od\_receipt\_time']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 427 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $app\_no\_subj; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 428 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $app\_no; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 439 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo get\_text($od['od\_deposit\_name']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 443 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo get\_text($od['od\_bank\_account']); ?></span>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 460 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

MD5 Hashing algorithm.

$LGD\_HASHDATA = md5($LGD\_MID.$LGD\_TID.$LGD\_MERTKEY);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 469 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $hp\_receipt\_script; ?>">영수증 출력</a>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 479 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

MD5 Hashing algorithm.

$LGD\_HASHDATA = md5($LGD\_MID.$LGD\_TID.$LGD\_MERTKEY);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 488 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $card\_receipt\_script; ?>">영수증 출력</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 497 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $card\_receipt\_script; ?>">영수증 출력</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 511 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo display\_point($od['od\_receipt\_point']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 522 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo display\_price($od['od\_refund\_price']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 563 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="<?php echo $cash\_receipt\_script; ?>" class="btn\_frmline">현금영수증 확인하기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 569 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:;" onclick="window.open('<?php echo G5\_SHOP\_URL; ?>/taxsave.php?od\_id=<?php echo $od\_id; ?>', 'taxsave', 'width=550,height=400,scrollbars=1,menus=0');" class="btn\_frmline is-long-text">현금영수증을 발급하시려면 클릭하십시오.</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 591 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="od\_id" value="<?php echo $od['od\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 592 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo $token; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 638 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="e\_trade\_no" value="<?php echo $od['od\_tno']; ?>"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 642 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="deposit\_no" value="<?php echo $deposit\_no; ?>"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 646 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\orderinquiryview.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><input type="text" name="req\_name" value="<?php echo $od['od\_deposit\_name']; ?>"></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="hd\_h1"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_SHOP\_URL; ?>/"><img src="<?php echo G5\_DATA\_URL; ?>/common/logo\_img" alt="<?php echo $config['cf\_title']; ?>"></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="q" value="<?php echo stripslashes(get\_text(get\_search\_string($q))); ?>" id="sch\_str" required placeholder="검색어를 입력해주세요">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 215 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="wrapper" class="<?php echo implode(' ', $wrapper\_class); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 237 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 260 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="<?php echo implode(' ', $content\_class); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 261 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.head.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ((!$bo\_table || $w == 's' ) && !defined('\_INDEX\_')) { ?><div id="wrapper\_title"><?php echo $g5['title'] ?></div><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>회사명</b> <?php echo $default['de\_admin\_company\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>주소</b> <?php echo $default['de\_admin\_company\_addr']; ?></span><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>사업자 등록번호</b> <?php echo $default['de\_admin\_company\_saupja\_no']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>대표</b> <?php echo $default['de\_admin\_company\_owner']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>전화</b> <?php echo $default['de\_admin\_company\_tel']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>팩스</b> <?php echo $default['de\_admin\_company\_fax']; ?></span><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <span><b>운영자</b> <?php echo $admin['mb\_name']; ?></span><br> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>통신판매업신고번호</b> <?php echo $default['de\_admin\_tongsin\_no']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><b>개인정보 보호책임자</b> <?php echo $default['de\_admin\_info\_name']; ?></span><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($default['de\_admin\_buga\_no']) echo '<span><b>부가통신사업신고번호</b> '.$default['de\_admin\_buga\_no'].'</span>'; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="ft\_copy">Copyright &copy; 2001-2013 <?php echo $default['de\_admin\_company\_name']; ?>. All Rights Reserved.</div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\shop.tail.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $config['cf\_analytics'];

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\shop\\_common.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$sort = preg\_replace("/[\<\>\'\"\\\'\\\"\%\=\(\)\s]/", "", $sort);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="bo\_list" style="width:<?php echo $width; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $board['bo\_subject'] ?> 카테고리</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>Total <?php echo number\_format($total\_count) ?>건</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $page ?> 페이지

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($admin\_href) { ?><li><a href="<?php echo $admin\_href ?>" class="btn\_admin btn" title="관리자"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($rss\_href) { ?><li><a href="<?php echo $rss\_href ?>" class="btn\_b01 btn" title="RSS"><i class="fa fa-rss" aria-hidden="true"></i><span class="sound\_only">RSS</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b01 btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $board['bo\_subject'] ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><?php echo subject\_sort\_link('wr\_hit', $qstr2, 1) ?>조회 </a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_good) { ?><th scope="col"><?php echo subject\_sort\_link('wr\_good', $qstr2, 1) ?>추천 </a></th><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_nogood) { ?><th scope="col"><?php echo subject\_sort\_link('wr\_nogood', $qstr2, 1) ?>비추천 </a></th><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="col"><?php echo subject\_sort\_link('wr\_datetime', $qstr2, 1) ?>날짜 </a></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php if ($list[$i]['is\_notice']) echo "bo\_notice"; ?> <?php echo $lt\_class ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_wr\_id[]" value="<?php echo $list[$i]['wr\_id'] ?>" id="chk\_wr\_id\_<?php echo $i ?>" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_wr\_id\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<b class="sound\_only"><?php echo $list[$i]['subject'] ?></b>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['num'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_subject" style="padding-left:<?php echo $list[$i]['reply'] ? (strlen($list[$i]['wr\_reply'])\*10) : '0'; ?>px">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['ca\_name\_href'] ?>" class="bo\_cate\_link"><?php echo $list[$i]['ca\_name'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['href'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['icon\_reply'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_secret'])) echo rtrim($list[$i]['icon\_secret']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['subject'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_hot'])) echo rtrim($list[$i]['icon\_hot']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_file'])) echo rtrim($list[$i]['icon\_file']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_link'])) echo rtrim($list[$i]['icon\_link']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['comment\_cnt']) { ?><span class="sound\_only">댓글</span><span class="cnt\_cmt"><?php echo $list[$i]['wr\_comment']; ?></span><span class="sound\_only">개</span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_name sv\_use"><?php echo $list[$i]['name'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 146 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $list[$i]['wr\_hit'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_good) { ?><td class="td\_num"><?php echo $list[$i]['wr\_good'] ?></td><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_nogood) { ?><td class="td\_num"><?php echo $list[$i]['wr\_nogood'] ?></td><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_datetime"><?php echo $list[$i]['datetime2'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (count($list) == 0) { echo '<tr><td colspan="'.$colspan.'" class="empty\_table">게시물이 없습니다.</td></tr>'; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($admin\_href) { ?><li><a href="<?php echo $admin\_href ?>" class="btn\_admin btn" title="관리자"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($rss\_href) { ?><li><a href="<?php echo $rss\_href ?>" class="btn\_b01 btn" title="RSS"><i class="fa fa-rss" aria-hidden="true"></i><span class="sound\_only">RSS</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 167 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b01 btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 179 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 184 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_board\_sfl\_select\_options($sfl); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 188 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo stripslashes($stx) ?>" required id="stx" class="sch\_input" size="25" maxlength="20" placeholder=" 검색어를 입력해주세요">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="bo\_v" style="width:<?php echo $width; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_cate"><?php echo $view['ca\_name'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo cut\_str(get\_text($view['wr\_subject']), 70);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="pf\_img"><?php echo get\_member\_profile\_img($view['mb\_id']) ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자</span> <strong><?php echo $view['name'] ?><?php if ($is\_ip\_view) { echo "&nbsp;($ip)"; } ?></strong><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">댓글</span><strong><a href="#bo\_vc"> <i class="fa fa-commenting-o" aria-hidden="true"></i> <?php echo number\_format($view['wr\_comment']) ?>건</a></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">조회</span><strong><i class="fa fa-eye" aria-hidden="true"></i> <?php echo number\_format($view['wr\_hit']) ?>회</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="if\_date"><span class="sound\_only">작성일</span><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo date("y-m-d H:i", strtotime($view['wr\_datetime'])) ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $list\_href ?>" class="btn\_b01 btn" title="목록"><i class="fa fa-list" aria-hidden="true"></i><span class="sound\_only">목록</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($reply\_href) { ?><li><a href="<?php echo $reply\_href ?>" class="btn\_b01 btn" title="답변"><i class="fa fa-reply" aria-hidden="true"></i><span class="sound\_only">답변</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b01 btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($update\_href) { ?><li><a href="<?php echo $update\_href ?>">수정<i class="fa fa-pencil-square-o" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($delete\_href) { ?><li><a href="<?php echo $delete\_href ?>" onclick="del(this.href); return false;">삭제<i class="fa fa-trash-o" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($copy\_href) { ?><li><a href="<?php echo $copy\_href ?>" onclick="board\_move(this.href); return false;">복사<i class="fa fa-files-o" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($move\_href) { ?><li><a href="<?php echo $move\_href ?>" onclick="board\_move(this.href); return false;">이동<i class="fa fa-arrows" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($search\_href) { ?><li><a href="<?php echo $search\_href ?>">검색<i class="fa fa-search" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($scrap\_href) { ?><a href="<?php echo $scrap\_href; ?>" target="\_blank" class="btn btn\_b03" onclick="win\_scrap(this.href); return false;"><i class="fa fa-bookmark" aria-hidden="true"></i> 스크랩</a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_file\_thumbnail($view\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="bo\_v\_con"><?php echo get\_view\_thumbnail($view['content']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_signature) { ?><p><?php echo $signature ?></p><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $good\_href.'&amp;'.$qstr ?>" id="good\_button" class="bo\_v\_good"><i class="fa fa-thumbs-o-up" aria-hidden="true"></i><span class="sound\_only">추천</span><strong><?php echo number\_format($view['wr\_good']) ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $nogood\_href.'&amp;'.$qstr ?>" id="nogood\_button" class="bo\_v\_nogood"><i class="fa fa-thumbs-o-down" aria-hidden="true"></i><span class="sound\_only">비추천</span><strong><?php echo number\_format($view['wr\_nogood']) ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($board['bo\_use\_good']) { ?><span class="bo\_v\_good"><i class="fa fa-thumbs-o-up" aria-hidden="true"></i><span class="sound\_only">추천</span><strong><?php echo number\_format($view['wr\_good']) ?></strong></span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($board['bo\_use\_nogood']) { ?><span class="bo\_v\_nogood"><i class="fa fa-thumbs-o-down" aria-hidden="true"></i><span class="sound\_only">비추천</span><strong><?php echo number\_format($view['wr\_nogood']) ?></strong></span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['file'][$i]['href']; ?>" class="view\_file\_download">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $view['file'][$i]['source'] ?></strong> <?php echo $view['file'][$i]['content'] ?> (<?php echo $view['file'][$i]['size'] ?>)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_file\_cnt"><?php echo $view['file'][$i]['download'] ?>회 다운로드 | DATE : <?php echo $view['file'][$i]['datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 194 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['link\_href'][$i] ?>" target="\_blank">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $link ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 198 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_link\_cnt"><?php echo $view['link\_hit'][$i] ?>회 연결</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 211 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($prev\_href) { ?><li class="btn\_prv"><span class="nb\_tit"><i class="fa fa-chevron-up" aria-hidden="true"></i> 이전글</span><a href="<?php echo $prev\_href ?>"><?php echo $prev\_wr\_subject;?></a> <span class="nb\_date"><?php echo str\_replace('-', '.', substr($prev\_wr\_date, '2', '8')); ?></span></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 212 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($next\_href) { ?><li class="btn\_next"><span class="nb\_tit"><i class="fa fa-chevron-down" aria-hidden="true"></i> 다음글</span><a href="<?php echo $next\_href ?>"><?php echo $next\_wr\_subject;?></a> <span class="nb\_date"><?php echo str\_replace('-', '.', substr($next\_wr\_date, '2', '8')); ?></span></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 232 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var msg = "파일을 다운로드 하시면 포인트가 차감(<?php echo number\_format($board['bo\_download\_point']) ?>점)됩니다.\n\n포인트는 게시물당 한번만 차감되며 다음에 다시 다운로드 하셔도 중복하여 차감하지 않습니다.\n\n그래도 다운로드 하시겠습니까?";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_min = parseInt(<?php echo $comment\_min ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_max = parseInt(<?php echo $comment\_max ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" class="cmt\_btn"><span class="total"><b>댓글</b> <?php echo $view['wr\_comment']; ?></span><span class="cmt\_more"></span></button>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$comment = preg\_replace("/\[\<a\s.\*href\=\"(http|https|ftp|mms)\:\/\/([^[:space:]]+)\.(mp3|wma|wmv|asf|asx|mpg|mpeg)\".\*\<\/a\>\]/i", "<script>doc\_write(obj\_movie('$1:

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="c\_<?php echo $comment\_id ?>" <?php if ($cmt\_depth) { ?>style="margin-left:<?php echo $cmt\_depth ?>px;border-top-color:#e0e0e0"<?php } ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="pf\_img"><?php echo get\_member\_profile\_img($list[$i]['mb\_id']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<header style="z-index:<?php echo $cmt\_sv; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo get\_text($list[$i]['wr\_name']); ?>님의 <?php if ($cmt\_depth) { ?><span class="sound\_only">댓글의</span><?php } ?> 댓글</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>(<?php echo $list[$i]['ip']; ?>)</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_vc\_hdinfo"><i class="fa fa-clock-o" aria-hidden="true"></i> <time datetime="<?php echo date('Y-m-d\TH:i:s+09:00', strtotime($list[$i]['datetime'])) ?>"><?php echo $list[$i]['datetime'] ?></time></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (strstr($list[$i]['wr\_option'], "secret")) { ?><img src="<?php echo $board\_skin\_url; ?>/img/icon\_secret.gif" alt="비밀글"><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $comment ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="edit\_<?php echo $comment\_id ?>" class="bo\_vc\_w"></span><!-- 수정 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="reply\_<?php echo $comment\_id ?>" class="bo\_vc\_w"></span><!-- 답변 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" value="<?php echo strstr($list[$i]['wr\_option'],"secret") ?>" id="secret\_comment\_<?php echo $comment\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea id="save\_comment\_<?php echo $comment\_id ?>" style="display:none"><?php echo get\_text($list[$i]['content1'], 0) ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_reply']) { ?><li><a href="<?php echo $c\_reply\_href; ?>" onclick="comment\_box('<?php echo $comment\_id ?>', 'c'); return false;">답변</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_edit']) { ?><li><a href="<?php echo $c\_edit\_href; ?>" onclick="comment\_box('<?php echo $comment\_id ?>', 'cu'); return false;">수정</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_del']) { ?><li><a href="<?php echo $list[$i]['del\_link']; ?>" onclick="return comment\_delete();">삭제</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fviewcomment" id="fviewcomment" action="<?php echo $comment\_action\_url; ?>" onsubmit="return fviewcomment\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>" id="w">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comment\_id" value="<?php echo $c\_id ?>" id="comment\_id">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($comment\_min || $comment\_max) { ?>onkeyup="check\_byte('wr\_content', 'char\_count');"<?php } ?>><?php echo $c\_wr\_content; ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_html; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 261 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($is\_guest) echo chk\_captcha\_js(); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 333 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

"<?php echo G5\_SNS\_URL; ?>/view\_comment\_write.sns.skin.php?bo\_table=<?php echo $bo\_table; ?>",

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="sound\_only"><?php echo $g5['title'] ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fwrite" id="fwrite" action="<?php echo $action\_url ?>" onsubmit="return fwrite\_submit(this);" method="post" enctype="multipart/form-data" autocomplete="off" style="width:<?php echo $width; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_hidden;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_name" value="<?php echo $name ?>" id="wr\_name" required class="frm\_input half\_input required" placeholder="이름">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="password" name="wr\_password" id="wr\_password" <?php echo $password\_required ?> class="frm\_input half\_input <?php echo $password\_required ?>" placeholder="비밀번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_email" value="<?php echo $email ?>" id="wr\_email" class="frm\_input half\_input email " placeholder="이메일">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_homepage" value="<?php echo $homepage ?>" id="wr\_homepage" class="frm\_input half\_input" size="50" placeholder="홈페이지">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_subject" value="<?php echo $subject ?>" id="wr\_subject" required class="frm\_input full\_input required" size="50" maxlength="255" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($editor\_content\_js) echo $editor\_content\_js; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" id="btn\_autosave" class="btn\_frmline">임시 저장된 글 (<span id="autosave\_count"><?php echo $autosave\_count; ?></span>)</button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="wr\_content <?php echo $is\_dhtml\_editor ? $config['cf\_editor'] : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p id="char\_count\_desc">이 게시판은 최소 <strong><?php echo $write\_min; ?></strong>글자 이상, 최대 <strong><?php echo $write\_max; ?></strong>글자 이하까지 글을 쓰실 수 있습니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="wr\_link<?php echo $i ?>"><i class="fa fa-link" aria-hidden="true"></i><span class="sound\_only"> 링크 #<?php echo $i ?></span></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_link<?php echo $i ?>" value="<?php if($w=="u"){ echo $write['wr\_link'.$i]; } ?>" id="wr\_link<?php echo $i ?>" class="frm\_input full\_input" size="50">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bf\_file\_<?php echo $i+1 ?>" class="lb\_icon"><i class="fa fa-folder-open" aria-hidden="true"></i><span class="sound\_only"> 파일 #<?php echo $i+1 ?></span></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="file" name="bf\_file[]" id="bf\_file\_<?php echo $i+1 ?>" title="파일첨부 <?php echo $i+1 ?> : 용량 <?php echo $upload\_max\_filesize ?> 이하만 업로드 가능" class="frm\_file ">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 144 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bf\_content[]" value="<?php echo ($w == 'u') ? $file[$i]['bf\_content'] : ''; ?>" title="파일 설명을 입력해주세요." class="full\_input frm\_input" size="50" placeholder="파일 설명을 입력해주세요.">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="bf\_file\_del<?php echo $i ?>" name="bf\_file\_del[<?php echo $i; ?>]" value="1"> <label for="bf\_file\_del<?php echo $i ?>"><?php echo $file[$i]['source'].'('.$file[$i]['size'].')'; ?> 파일 삭제</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_html ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="btn\_cancel btn">취소</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 172 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_min = parseInt(<?php echo $write\_min; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 173 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_max = parseInt(<?php echo $write\_max; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 198 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 247 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="bo\_gall" style="width:<?php echo $width; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $board['bo\_subject'] ?> 카테고리</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>Total <?php echo number\_format($total\_count) ?>건</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $page ?> 페이지

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($admin\_href) { ?><li><a href="<?php echo $admin\_href ?>" class="btn\_admin btn" title="관리자"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($rss\_href) { ?><li><a href="<?php echo $rss\_href ?>" class="btn\_b01 btn" title="RSS"><i class="fa fa-rss" aria-hidden="true"></i><span class="sound\_only">RSS</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b01 btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php echo implode(' ', $classes); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_wr\_id[]" value="<?php echo $list[$i]['wr\_id'] ?>" id="chk\_wr\_id\_<?php echo $i ?>" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_wr\_id\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<b class="sound\_only"><?php echo $list[$i]['subject'] ?></b>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['num'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="gall\_img" style="<?php if ($board['bo\_gallery\_height'] > 0) echo 'height:'.$board['bo\_gallery\_height'].'px;max-height:'.$board['bo\_gallery\_height'].'px'; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['href'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="is\_notice" style="<?php echo $line\_height\_style; ?>">공지</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo run\_replace('thumb\_image\_tag', $img\_content, $thumb);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['ca\_name\_href'] ?>" class="bo\_cate\_link"><?php echo $list[$i]['ca\_name'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['href'] ?>" class="bo\_tit">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['subject'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_hot'])) echo rtrim($list[$i]['icon\_hot']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_secret'])) echo rtrim($list[$i]['icon\_secret']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['comment\_cnt']) { ?><span class="sound\_only">댓글</span><span class="cnt\_cmt"><?php echo $list[$i]['wr\_comment']; ?></span><span class="sound\_only">개</span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 153 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자 </span><?php echo $list[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="gall\_date"><span class="sound\_only">작성일 </span><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$i]['datetime2'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 155 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="gall\_view"><span class="sound\_only">조회 </span><i class="fa fa-eye" aria-hidden="true"></i> <?php echo $list[$i]['wr\_hit'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_good) { ?><span class="sound\_only">추천</span><strong><i class="fa fa-thumbs-o-up" aria-hidden="true"></i> <?php echo $list[$i]['wr\_good'] ?></strong><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_nogood) { ?><span class="sound\_only">비추천</span><strong><i class="fa fa-thumbs-o-down" aria-hidden="true"></i> <?php echo $list[$i]['wr\_nogood'] ?></strong><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (count($list) == 0) { echo "<li class=\"empty\_list\">게시물이 없습니다.</li>"; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 169 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 176 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($admin\_href) { ?><li><a href="<?php echo $admin\_href ?>" class="btn\_admin btn" title="관리자"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 177 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($rss\_href) { ?><li><a href="<?php echo $rss\_href ?>" class="btn\_b01 btn" title="RSS"><i class="fa fa-rss" aria-hidden="true"></i><span class="sound\_only">RSS</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 178 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b01 btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 190 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 191 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_board\_sfl\_select\_options($sfl); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 199 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo stripslashes($stx) ?>" required id="stx" class="sch\_input" size="25" maxlength="20" placeholder="검색어를 입력해주세요">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="bo\_v" style="width:<?php echo $width; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_cate"><?php echo $view['ca\_name'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo cut\_str(get\_text($view['wr\_subject']), 70);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="pf\_img"><?php echo get\_member\_profile\_img($view['mb\_id']) ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자</span> <strong><?php echo $view['name'] ?><?php if ($is\_ip\_view) { echo "&nbsp;($ip)"; } ?></strong><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">댓글</span><strong><a href="#bo\_vc"> <i class="fa fa-commenting-o" aria-hidden="true"></i> <?php echo number\_format($view['wr\_comment']) ?>건</a></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">조회</span><strong><i class="fa fa-eye" aria-hidden="true"></i> <?php echo number\_format($view['wr\_hit']) ?>회</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="if\_date"><span class="sound\_only">작성일</span><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo date("y-m-d H:i", strtotime($view['wr\_datetime'])) ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $list\_href ?>" class="btn\_b01 btn" title="목록"><i class="fa fa-list" aria-hidden="true"></i><span class="sound\_only">목록</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($reply\_href) { ?><li><a href="<?php echo $reply\_href ?>" class="btn\_b01 btn" title="답변"><i class="fa fa-reply" aria-hidden="true"></i><span class="sound\_only">답변</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b01 btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($update\_href) { ?><li><a href="<?php echo $update\_href ?>">수정<i class="fa fa-pencil-square-o" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($delete\_href) { ?><li><a href="<?php echo $delete\_href ?>" onclick="del(this.href); return false;">삭제<i class="fa fa-trash-o" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($copy\_href) { ?><li><a href="<?php echo $copy\_href ?>" onclick="board\_move(this.href); return false;">복사<i class="fa fa-files-o" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($move\_href) { ?><li><a href="<?php echo $move\_href ?>" onclick="board\_move(this.href); return false;">이동<i class="fa fa-arrows" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($search\_href) { ?><li><a href="<?php echo $search\_href ?>">검색<i class="fa fa-search" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($scrap\_href) { ?><a href="<?php echo $scrap\_href; ?>" target="\_blank" class="btn btn\_b03" onclick="win\_scrap(this.href); return false;"><i class="fa fa-bookmark" aria-hidden="true"></i> 스크랩</a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_file\_thumbnail($view\_file);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="bo\_v\_con"><?php echo get\_view\_thumbnail($view['content']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_signature) { ?><p><?php echo $signature ?></p><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $good\_href.'&amp;'.$qstr ?>" id="good\_button" class="bo\_v\_good"><i class="fa fa-thumbs-o-up" aria-hidden="true"></i><span class="sound\_only">추천</span><strong><?php echo number\_format($view['wr\_good']) ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $nogood\_href.'&amp;'.$qstr ?>" id="nogood\_button" class="bo\_v\_nogood"><i class="fa fa-thumbs-o-down" aria-hidden="true"></i><span class="sound\_only">비추천</span><strong><?php echo number\_format($view['wr\_nogood']) ?></strong></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($board['bo\_use\_good']) { ?><span class="bo\_v\_good"><i class="fa fa-thumbs-o-up" aria-hidden="true"></i><span class="sound\_only">추천</span><strong><?php echo number\_format($view['wr\_good']) ?></strong></span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($board['bo\_use\_nogood']) { ?><span class="bo\_v\_nogood"><i class="fa fa-thumbs-o-down" aria-hidden="true"></i><span class="sound\_only">비추천</span><strong><?php echo number\_format($view['wr\_nogood']) ?></strong></span><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 164 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['file'][$i]['href']; ?>" class="view\_file\_download">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $view['file'][$i]['source'] ?></strong> <?php echo $view['file'][$i]['content'] ?> (<?php echo $view['file'][$i]['size'] ?>)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_file\_cnt"><?php echo $view['file'][$i]['download'] ?>회 다운로드 | DATE : <?php echo $view['file'][$i]['datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 194 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['link\_href'][$i] ?>" target="\_blank">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 195 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $link ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 198 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_v\_link\_cnt"><?php echo $view['link\_hit'][$i] ?>회 연결</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 211 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($prev\_href) { ?><li class="btn\_prv"><span class="nb\_tit"><i class="fa fa-chevron-up" aria-hidden="true"></i> 이전글</span><a href="<?php echo $prev\_href ?>"><?php echo $prev\_wr\_subject;?></a> <span class="nb\_date"><?php echo str\_replace('-', '.', substr($prev\_wr\_date, '2', '8')); ?></span></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 212 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($next\_href) { ?><li class="btn\_next"><span class="nb\_tit"><i class="fa fa-chevron-down" aria-hidden="true"></i> 다음글</span><a href="<?php echo $next\_href ?>"><?php echo $next\_wr\_subject;?></a> <span class="nb\_date"><?php echo str\_replace('-', '.', substr($next\_wr\_date, '2', '8')); ?></span></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 232 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var msg = "파일을 다운로드 하시면 포인트가 차감(<?php echo number\_format($board['bo\_download\_point']) ?>점)됩니다.\n\n포인트는 게시물당 한번만 차감되며 다음에 다시 다운로드 하셔도 중복하여 차감하지 않습니다.\n\n그래도 다운로드 하시겠습니까?";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 7 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_min = parseInt(<?php echo $comment\_min ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_max = parseInt(<?php echo $comment\_max ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" class="cmt\_btn"><span class="total"><b>댓글</b> <?php echo $view['wr\_comment']; ?></span><span class="cmt\_more"></span></button>

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$comment = preg\_replace("/\[\<a\s.\*href\=\"(http|https|ftp|mms)\:\/\/([^[:space:]]+)\.(mp3|wma|wmv|asf|asx|mpg|mpeg)\".\*\<\/a\>\]/i", "<script>doc\_write(obj\_movie('$1:

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="c\_<?php echo $comment\_id ?>" <?php if ($cmt\_depth) { ?>style="margin-left:<?php echo $cmt\_depth ?>px;border-top-color:#e0e0e0"<?php } ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="pf\_img"><?php echo get\_member\_profile\_img($list[$i]['mb\_id']) ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<header style="z-index:<?php echo $cmt\_sv; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo get\_text($list[$i]['wr\_name']); ?>님의 <?php if ($cmt\_depth) { ?><span class="sound\_only">댓글의</span><?php } ?> 댓글</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>(<?php echo $list[$i]['ip']; ?>)</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_vc\_hdinfo"><i class="fa fa-clock-o" aria-hidden="true"></i> <time datetime="<?php echo date('Y-m-d\TH:i:s+09:00', strtotime($list[$i]['datetime'])) ?>"><?php echo $list[$i]['datetime'] ?></time></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (strstr($list[$i]['wr\_option'], "secret")) { ?><img src="<?php echo $board\_skin\_url; ?>/img/icon\_secret.gif" alt="비밀글"><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $comment ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="edit\_<?php echo $comment\_id ?>" class="bo\_vc\_w"></span><!-- 수정 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="reply\_<?php echo $comment\_id ?>" class="bo\_vc\_w"></span><!-- 답변 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" value="<?php echo strstr($list[$i]['wr\_option'],"secret") ?>" id="secret\_comment\_<?php echo $comment\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea id="save\_comment\_<?php echo $comment\_id ?>" style="display:none"><?php echo get\_text($list[$i]['content1'], 0) ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_reply']) { ?><li><a href="<?php echo $c\_reply\_href; ?>" onclick="comment\_box('<?php echo $comment\_id ?>', 'c'); return false;">답변</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_edit']) { ?><li><a href="<?php echo $c\_edit\_href; ?>" onclick="comment\_box('<?php echo $comment\_id ?>', 'cu'); return false;">수정</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['is\_del']) { ?><li><a href="<?php echo $list[$i]['del\_link']; ?>" onclick="return comment\_delete();">삭제</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fviewcomment" id="fviewcomment" action="<?php echo $comment\_action\_url; ?>" onsubmit="return fviewcomment\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>" id="w">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comment\_id" value="<?php echo $c\_id ?>" id="comment\_id">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($comment\_min || $comment\_max) { ?>onkeyup="check\_byte('wr\_content', 'char\_count');"<?php } ?>><?php echo $c\_wr\_content; ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_html; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 262 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($is\_guest) echo chk\_captcha\_js(); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 334 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\view\_comment.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

"<?php echo G5\_SNS\_URL; ?>/view\_comment\_write.sns.skin.php?bo\_table=<?php echo $bo\_table; ?>",

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="sound\_only"><?php echo $g5['title'] ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fwrite" id="fwrite" action="<?php echo $action\_url ?>" onsubmit="return fwrite\_submit(this);" method="post" enctype="multipart/form-data" autocomplete="off" style="width:<?php echo $width; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="spt" value="<?php echo $spt ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sst" value="<?php echo $sst ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sod" value="<?php echo $sod ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_hidden;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_name" value="<?php echo $name ?>" id="wr\_name" required class="frm\_input half\_input required" placeholder="이름">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="password" name="wr\_password" id="wr\_password" <?php echo $password\_required ?> class="frm\_input half\_input <?php echo $password\_required ?>" placeholder="비밀번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_email" value="<?php echo $email ?>" id="wr\_email" class="frm\_input half\_input email " placeholder="이메일">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_homepage" value="<?php echo $homepage ?>" id="wr\_homepage" class="frm\_input half\_input" size="50" placeholder="홈페이지">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_subject" value="<?php echo $subject ?>" id="wr\_subject" required class="frm\_input full\_input required" size="50" maxlength="255" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if($editor\_content\_js) echo $editor\_content\_js; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" id="btn\_autosave" class="btn\_frmline">임시 저장된 글 (<span id="autosave\_count"><?php echo $autosave\_count; ?></span>)</button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="wr\_content <?php echo $is\_dhtml\_editor ? $config['cf\_editor'] : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p id="char\_count\_desc">이 게시판은 최소 <strong><?php echo $write\_min; ?></strong>글자 이상, 최대 <strong><?php echo $write\_max; ?></strong>글자 이하까지 글을 쓰실 수 있습니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="wr\_link<?php echo $i ?>"><i class="fa fa-link" aria-hidden="true"></i><span class="sound\_only"> 링크 #<?php echo $i ?></span></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="wr\_link<?php echo $i ?>" value="<?php if($w=="u"){ echo $write['wr\_link'.$i]; } ?>" id="wr\_link<?php echo $i ?>" class="frm\_input full\_input" size="50">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="bf\_file\_<?php echo $i+1 ?>" class="lb\_icon"><i class="fa fa-folder-open" aria-hidden="true"></i><span class="sound\_only"> 파일 #<?php echo $i+1 ?></span></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="file" name="bf\_file[]" id="bf\_file\_<?php echo $i+1 ?>" title="파일첨부 <?php echo $i+1 ?> : 용량 <?php echo $upload\_max\_filesize ?> 이하만 업로드 가능" class="frm\_file ">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="bf\_content[]" value="<?php echo ($w == 'u') ? $file[$i]['bf\_content'] : ''; ?>" title="파일 설명을 입력해주세요." class="full\_input frm\_input" size="50" placeholder="파일 설명을 입력해주세요.">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="bf\_file\_del<?php echo $i ?>" name="bf\_file\_del[<?php echo $i; ?>]" value="1"> <label for="bf\_file\_del<?php echo $i ?>"><?php echo $file[$i]['source'].'('.$file[$i]['size'].')'; ?> 파일 삭제</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 157 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_html ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="btn\_cancel btn">취소</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 170 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_min = parseInt(<?php echo $write\_min; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var char\_max = parseInt(<?php echo $write\_max; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 196 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 245 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\board\gallery\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $captcha\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\connect\basic\connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $row['total\_cnt'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\connect\basic\current\_connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="crt\_num"><?php echo $list[$i]['num'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\connect\basic\current\_connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="crt\_profile"><?php echo get\_member\_profile\_img($list[$i]['mb\_id']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\connect\basic\current\_connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="crt\_name"><?php echo $list[$i]['name'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\connect\basic\current\_connect.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="crt\_lct"><?php echo $display\_location ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\content\basic\content.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<article id="ctt" class="ctt\_<?php echo $co\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\content\basic\content.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title']; ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\content\basic\content.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="faq\_himg" class="faq\_img"><img src="'.$himg\_src.'" alt=""></div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="faq\_hhtml">'.conv\_content($fm['fm\_head\_html'], 1).'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fm\_id" value="<?php echo $fm\_id;?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx;?>" required id="stx" class="frm\_input" size="15" maxlength="15">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $category\_href;?>?fm\_id=<?php echo $v['fm\_id'];?>" <?php echo $category\_option;?> ><?php echo $category\_msg.$v['fm\_subject'];?></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="faq\_wrap" class="faq\_<?php echo $fm\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $g5['title']; ?> 목록</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="tit\_bg">Q</span><a href="#none" onclick="return faq\_open(this);"><?php echo conv\_content($v['fa\_subject'], 1); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($v['fa\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($page\_rows, $page, $total\_page, $\_SERVER['SCRIPT\_NAME'].'?'.$qstr.'&amp;page='); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="faq\_thtml">'.conv\_content($fm['fm\_tail\_html'], 1).'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div id="faq\_timg" class="faq\_img"><img src="'.$timg\_src.'" alt=""></div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\faq\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="faq\_admin"><a href="'.$admin\_href.'" class="btn\_admin btn" title="FAQ 수정"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">FAQ 수정</span></a></div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="lat\_title"><a href="<?php echo get\_pretty\_url($bo\_table); ?>"><?php echo $bo\_subject ?></a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_secret']) echo "<i class=\"fa fa-lock\" aria-hidden=\"true\"></i><span class=\"sound\_only\">비밀글</span> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".get\_pretty\_url($bo\_table, $list[$i]['wr\_id'])."\"> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strong>".$list[$i]['subject']."</strong>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_hot']) echo "<span class=\"hot\_icon\"><i class=\"fa fa-heart\" aria-hidden=\"true\"></i><span class=\"sound\_only\">인기글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['icon\_reply']." ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_file']) && $list[$i]['icon\_file']) echo " <i class=\"fa fa-download\" aria-hidden=\"true\"></i>" ;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_link']) echo " <i class=\"fa fa-link\" aria-hidden=\"true\"></i>" ;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['comment\_cnt']) echo "

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="lt\_nick"><?php echo $list[$i]['name'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="lt\_date"><?php echo $list[$i]['datetime2'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="lt\_more"><span class="sound\_only"><?php echo $bo\_subject ?></span>더보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><a href="<?php echo get\_pretty\_url($bo\_table); ?>"><?php echo $bo\_subject ?></a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_secret']) echo "<span class=\"lock\_icon\"><i class=\"fa fa-lock\" aria-hidden=\"true\"></i></span> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".get\_pretty\_url($bo\_table, $list[$i]['wr\_id'])."\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strong>".$list[$i]['subject']."</strong>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\notice\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['comment\_cnt'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="lat\_title"><a href="<?php echo get\_pretty\_url($bo\_table); ?>"><?php echo $bo\_subject ?></a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['href'] ?>" class="lt\_img"><?php echo $img\_content; ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_secret']) echo "<i class=\"fa fa-lock\" aria-hidden=\"true\"></i><span class=\"sound\_only\">비밀글</span> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_hot']) echo "<span class=\"hot\_icon\">H<span class=\"sound\_only\">인기글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".$list[$i]['href']."\"> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strong>".$list[$i]['subject']."</strong>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['comment\_cnt']) echo "

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="lt\_date"><?php echo $list[$i]['datetime2'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="lt\_more"><span class="sound\_only"><?php echo $bo\_subject ?></span><i class="fa fa-plus" aria-hidden="true"></i><span class="sound\_only"> 더보기</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="lat\_title"><a href="<?php echo get\_pretty\_url($bo\_table); ?>"><?php echo $bo\_subject ?></a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $wr\_href; ?>" class="lt\_img"><?php echo run\_replace('thumb\_image\_tag', $img\_content, $thumb); ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_secret']) echo "<i class=\"fa fa-lock\" aria-hidden=\"true\"></i><span class=\"sound\_only\">비밀글</span> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".$wr\_href."\"> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strong>".$list[$i]['subject']."</strong>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_hot']) echo "<span class=\"hot\_icon\">H<span class=\"sound\_only\">인기글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['comment\_cnt']) echo "

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="lt\_nick"><?php echo $list[$i]['name'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="lt\_date"><?php echo $list[$i]['datetime2'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_block\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="lt\_more"><span class="sound\_only"><?php echo $bo\_subject ?></span>더보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="lat\_title"><a href="<?php echo get\_pretty\_url($bo\_table); ?>"><?php echo $bo\_subject ?></a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $img\_link\_html; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_secret']) echo "<i class=\"fa fa-lock\" aria-hidden=\"true\"></i><span class=\"sound\_only\">비밀글</span> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".$wr\_href."\" class=\"pic\_li\_tit\"> ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strong>".$list[$i]['subject']."</strong>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_new']) echo "<span class=\"new\_icon\">N<span class=\"sound\_only\">새글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['icon\_hot']) echo "<span class=\"hot\_icon\">H<span class=\"sound\_only\">인기글</span></span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($list[$i]['comment\_cnt']) echo "

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="lt\_nick"><?php echo $list[$i]['name'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="lt\_date"><?php echo $list[$i]['datetime2'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\pic\_list\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($bo\_table); ?>" class="lt\_more"><span class="sound\_only"><?php echo $bo\_subject ?></span>더보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="lat\_title"><i class="fa fa-list-ul" aria-hidden="true"></i> <a href="<?php echo G5\_BBS\_URL ?>/board.php?bo\_table=<?php echo $bo\_table ?>"><?php echo $bo\_subject ?></a></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"".$list[$i]['href']."\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strong>".$list[$i]['subject']."</strong>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list[$i]['comment\_cnt'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\latest\shop\_basic\latest.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (isset($list[$i]['icon\_new']) && $list[$i]['icon\_new']) echo " <span class=\"new\_icon\">NEW</span>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\formmail.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $name ?>님께 메일보내기</h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\formmail.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="to" value="<?php echo $email ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\formmail.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fnick" value="<?php echo get\_text($member['mb\_nick']) ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\formmail.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="fmail" value="<?php echo $member['mb\_email'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="flogin" action="<?php echo $login\_action\_url ?>" onsubmit="return flogin\_submit(this);" method="post">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="url" value="<?php echo $login\_url ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($default['de\_guest\_privacy'], $config['cf\_editor']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

f.url.value = "<?php echo $url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

f.action = "<?php echo $url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="forderinquiry" method="post" action="<?php echo urldecode($url); ?>" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\login.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="od\_id" value="<?php echo get\_text($od\_id); ?>" id="od\_id" required class="frm\_input required" size="20" placeholder="주문서번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fcertrefreshform" id="member\_cert\_refresh" action="<?php echo $action\_url ?>" onsubmit="return fcertrefreshform\_submit(this);" method="POST" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cert\_type" value="<?php echo $member['mb\_certify']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $member['mb\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_hp" value="<?php echo $member['mb\_hp']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_name" value="<?php echo $member['mb\_name']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td>생년월일<?php echo (empty($member['mb\_dupinfo']))? ", 휴대폰 번호(아이핀 제외)" : ""; ?>, 암호화된 개인식별부호(CI)</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\member\_cert\_refresh.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

certify\_win\_open("<?php echo $cert\_type; ?>", "<?php echo $cert\_url; ?>" + params);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\member\_confirm.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\member\_confirm.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fmemberconfirm" action="<?php echo $url ?>" onsubmit="return fmemberconfirm\_submit(this);" method="post">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\member\_confirm.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_id" value="<?php echo $member['mb\_id'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\member\_confirm.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="mb\_confirm\_id"><?php echo $member['mb\_id'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $g5['title'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="win\_total">전체 <?php echo $kind\_title ?>쪽지 <?php echo $total\_count ?>통<br></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php echo $readed; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($list[$i]['mb\_id']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['name']; ?> <span class="memo\_datetime"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$i]['send\_datetime']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['view\_href']; ?>"><?php echo $memo\_preview; ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['del\_href']; ?>" onclick="del(this.href); return false;" class="memo\_del"><i class="fa fa-trash-o" aria-hidden="true"></i> <span class="sound\_only">삭제</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($i==0) { echo '<li class="empty\_table">자료가 없습니다.</li>'; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p class="win\_desc"><i class="fa fa-info-circle" aria-hidden="true"></i> 쪽지 보관일수는 최장 <strong><?php echo $config['cf\_memo\_del'] ?></strong>일 입니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fmemoform" action="<?php echo $memo\_action\_url; ?>" onsubmit="return fmemoform\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="me\_recv\_mb\_id" value="<?php echo $me\_recv\_mb\_id; ?>" id="me\_recv\_mb\_id" required class="frm\_input full\_input required" size="47" placeholder="받는 회원아이디">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<br ><span class="frm\_info">쪽지 보낼때 회원당 <?php echo number\_format($config['cf\_memo\_send\_point']); ?>점의 포인트를 차감합니다.</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="me\_memo" id="me\_memo" required class="required"><?php echo $content ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($mb['mb\_id']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="memo\_view\_nick"><?php echo $nick ?></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="memo\_view\_date"><span class="sound\_only"><?php echo $kind\_date ?>시간</span><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $memo['me\_send\_datetime'] ?></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="memo\_op\_btn list\_btn"><a href="<?php echo $list\_link ?>" class="btn\_b01 btn"><i class="fa fa-list" aria-hidden="true"></i><span class="sound\_only">목록</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="memo\_op\_btn del\_btn"><a href="<?php echo $del\_link; ?>" onclick="del(this.href); return false;" class="memo\_del btn\_b01 btn"><i class="fa fa-trash-o" aria-hidden="true"></i> <span class="sound\_only">삭제</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $prev\_link ?>" class="btn\_left"><i class="fa fa-chevron-left" aria-hidden="true"></i> 이전쪽지</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $next\_link ?>" class="btn\_right">다음쪽지 <i class="fa fa-chevron-right" aria-hidden="true"></i></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($memo['me\_memo'], 0) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\memo\_view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($kind == 'recv') { ?><a href="./memo\_form.php?me\_recv\_mb\_id=<?php echo $mb['mb\_id'] ?>&amp;me\_id=<?php echo $memo['me\_id'] ?>" class="reply\_btn">답장</a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fboardpassword" action="<?php echo $action; ?>" method="post">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="comment\_id" value="<?php echo $comment\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\password.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\password\_lost.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fpasswordlost" action="<?php echo $action\_url ?>" onsubmit="return fpasswordlost\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\password\_lost.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

certify\_win\_open("<?php echo $cert\_type; ?>", "<?php echo $cert\_url; ?>"+params);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\password\_reset.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fpasswordreset" action="<?php echo $action\_url; ?>" onsubmit="return fpasswordreset\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\password\_reset.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_id" id="mb\_id" value="<?php echo $\_POST['mb\_id']; ?>" required class="required frm\_input full\_input" size="30" placeholder="아이디" readonly>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo number\_format($member['mb\_point']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php echo $point\_use\_class; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="point\_tit"><?php echo $po\_content; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="point\_num"><?php if ($point1) echo $point1; else echo $point2; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="point\_date1"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $row['po\_datetime']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="point\_date<?php echo $expr; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

만료 <?php echo substr(str\_replace('-', '', $row['po\_expire\_date']), 2); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php } else echo $row['po\_expire\_date'] == '9999-12-31' ? '&nbsp;' : $row['po\_expire\_date']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $sum\_point1; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $sum\_point2; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\point.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging(G5\_IS\_MOBILE ? $config['cf\_mobile\_pages'] : $config['cf\_write\_pages'], $page, $total\_page, $\_SERVER['SCRIPT\_NAME'].'?'.$qstr.'&amp;page='); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $mb\_nick ?>님의 프로필</h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($mb['mb\_id']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $mb\_nick ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $mb['mb\_level'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($mb['mb\_point']) ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo ($member['mb\_level'] >= $mb['mb\_level']) ? substr($mb['mb\_datetime'],0,10) ." (".number\_format($mb\_reg\_after)." 일)" : "알 수 없음"; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo ($member['mb\_level'] >= $mb['mb\_level']) ? $mb['mb\_today\_login'] : "알 수 없음"; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td colspan="3"><a href="<?php echo $mb\_homepage ?>" target="\_blank"><?php echo $mb\_homepage ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\profile.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo $mb\_profile ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fregister" id="fregister" action="<?php echo $register\_action\_url ?>" onsubmit="return fregister\_submit(this);" method="POST" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea readonly><?php echo get\_text($config['cf\_stipulation']) ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td>아이디, 이름, 비밀번호<?php echo ($config['cf\_cert\_use'])? ", 생년월일, 휴대폰 번호(본인인증 할 때만, 아이핀 제외), 암호화된 개인식별부호(CI)" : ""; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form id="fregisterform" name="fregisterform" action="<?php echo $register\_action\_url ?>" onsubmit="return fregisterform\_submit(this);" method="post" enctype="multipart/form-data" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="agree" value="<?php echo $agree ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="agree2" value="<?php echo $agree2 ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="cert\_type" value="<?php echo $member['mb\_certify']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if (isset($member['mb\_sex'])) { ?><input type="hidden" name="mb\_sex" value="<?php echo $member['mb\_sex'] ?>"><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_nick\_default" value="<?php echo get\_text($member['mb\_nick']) ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_nick" value="<?php echo get\_text($member['mb\_nick']) ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_id" value="<?php echo $member['mb\_id'] ?>" id="reg\_mb\_id" <?php echo $required ?> <?php echo $readonly ?> class="frm\_input full\_input <?php echo $required ?> <?php echo $readonly ?>" minlength="3" maxlength="20" placeholder="아이디">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="password" name="mb\_password" id="reg\_mb\_password" <?php echo $required ?> class="frm\_input full\_input <?php echo $required ?>" minlength="3" maxlength="20" placeholder="비밀번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="password" name="mb\_password\_re" id="reg\_mb\_password\_re" <?php echo $required ?> class="frm\_input full\_input <?php echo $required ?>" minlength="3" maxlength="20" placeholder="비밀번호 확인">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $mb\_cert; ?> 본인확인</strong><?php if ($member['mb\_adult']) { ?> 및 <strong>성인인증</strong><?php } ?> 완료

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="reg\_mb\_name">이름 (필수)<?php echo $desc\_name ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" id="reg\_mb\_name" name="mb\_name" value="<?php echo get\_text($member['mb\_name']) ?>" <?php echo $required ?> <?php echo $readonly; ?> class="frm\_input full\_input <?php echo $required ?> <?php echo $name\_readonly ?>" size="10" placeholder="이름">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="tooltip">공백없이 한글,영문,숫자만 입력 가능 (한글2자, 영문4자 이상)<br> 닉네임을 바꾸시면 앞으로 <?php echo (int)$config['cf\_nick\_modify'] ?>일 이내에는 변경 할 수 없습니다.</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_nick\_default" value="<?php echo isset($member['mb\_nick'])?get\_text($member['mb\_nick']):''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_nick" value="<?php echo isset($member['mb\_nick'])?get\_text($member['mb\_nick']):''; ?>" id="reg\_mb\_nick" required class="frm\_input required nospace full\_input" size="10" maxlength="20" placeholder="닉네임">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($w=='') { echo "E-mail 로 발송된 내용을 확인한 후 인증하셔야 회원가입이 완료됩니다."; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($w=='u') { echo "E-mail 주소를 변경하시면 다시 인증하셔야 합니다."; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="old\_email" value="<?php echo $member['mb\_email'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_email" value="<?php echo isset($member['mb\_email'])?$member['mb\_email']:''; ?>" id="reg\_mb\_email" required class="frm\_input email full\_input required" size="70" maxlength="100" placeholder="E-mail">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_homepage" value="<?php echo get\_text($member['mb\_homepage']) ?>" id="reg\_mb\_homepage" <?php echo $config['cf\_req\_homepage']?"required":""; ?> class="frm\_input full\_input <?php echo $config['cf\_req\_homepage']?"required":""; ?>" size="70" maxlength="255" placeholder="홈페이지">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_tel" value="<?php echo get\_text($member['mb\_tel']) ?>" id="reg\_mb\_tel" <?php echo $config['cf\_req\_tel']?"required":""; ?> class="frm\_input full\_input <?php echo $config['cf\_req\_tel']?"required":""; ?>" maxlength="20" placeholder="전화번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="reg\_mb\_hp">휴대폰번호<?php if (!empty($hp\_required)) { ?> (필수)<?php } ?><?php echo $desc\_phone ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_hp" value="<?php echo get\_text($member['mb\_hp']) ?>" id="reg\_mb\_hp" <?php echo $hp\_required; ?> <?php echo $hp\_readonly; ?> class="frm\_input full\_input <?php echo $hp\_required; ?> <?php echo $hp\_readonly; ?>" maxlength="20" placeholder="휴대폰번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="old\_mb\_hp" value="<?php echo get\_text($member['mb\_hp']) ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 158 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="reg\_mb\_zip" class="sound\_only">우편번호<?php echo $config['cf\_req\_addr']?' (필수)':''; ?></label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_zip" value="<?php echo $member['mb\_zip1'].$member['mb\_zip2']; ?>" id="reg\_mb\_zip" <?php echo $config['cf\_req\_addr']?"required":""; ?> class="frm\_input twopart\_input <?php echo $config['cf\_req\_addr']?"required":""; ?>" size="5" maxlength="6" placeholder="우편번호">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_addr1" value="<?php echo get\_text($member['mb\_addr1']) ?>" id="reg\_mb\_addr1" <?php echo $config['cf\_req\_addr']?"required":""; ?> class="frm\_input frm\_address full\_input <?php echo $config['cf\_req\_addr']?"required":""; ?>" size="50" placeholder="기본주소">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="reg\_mb\_addr1" class="sound\_only">기본주소<?php echo $config['cf\_req\_addr']?' (필수)':''; ?></label><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 163 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_addr2" value="<?php echo get\_text($member['mb\_addr2']) ?>" id="reg\_mb\_addr2" class="frm\_input frm\_address full\_input" size="50" placeholder="상세주소">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_addr3" value="<?php echo get\_text($member['mb\_addr3']) ?>" id="reg\_mb\_addr3" class="frm\_input frm\_address full\_input" size="50" readonly="readonly" placeholder="참고항목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 168 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_addr\_jibeon" value="<?php echo get\_text($member['mb\_addr\_jibeon']); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="mb\_signature" id="reg\_mb\_signature" <?php echo $config['cf\_req\_signature']?"required":""; ?> class="<?php echo $config['cf\_req\_signature']?"required":""; ?>" placeholder="서명"><?php echo $member['mb\_signature'] ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<textarea name="mb\_profile" id="reg\_mb\_profile" <?php echo $config['cf\_req\_profile']?"required":""; ?> class="<?php echo $config['cf\_req\_profile']?"required":""; ?>" placeholder="자기소개"><?php echo $member['mb\_profile'] ?></textarea>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 196 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="tooltip">이미지 크기는 가로 <?php echo $config['cf\_member\_icon\_width'] ?>픽셀, 세로 <?php echo $config['cf\_member\_icon\_height'] ?>픽셀 이하로 해주세요.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 197 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

gif, jpg, png파일만 가능하며 용량 <?php echo number\_format($config['cf\_member\_icon\_size']) ?>바이트 이하만 등록됩니다.</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 202 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<img src="<?php echo $mb\_icon\_url ?>" alt="회원아이콘">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 215 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="tooltip">이미지 크기는 가로 <?php echo $config['cf\_member\_img\_width'] ?>픽셀, 세로 <?php echo $config['cf\_member\_img\_height'] ?>픽셀 이하로 해주세요.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 216 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

gif, jpg, png파일만 가능하며 용량 <?php echo number\_format($config['cf\_member\_img\_size']) ?>바이트 이하만 등록됩니다.</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 221 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<img src="<?php echo $mb\_img\_url ?>" alt="회원이미지">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 230 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="mb\_mailling" value="1" id="reg\_mb\_mailling" <?php echo ($w=='' || $member['mb\_mailling'])?'checked':''; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 240 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="mb\_sms" value="1" id="reg\_mb\_sms" <?php echo ($w=='' || $member['mb\_sms'])?'checked':''; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 251 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="mb\_open" value="1" id="reg\_mb\_open" <?php echo ($w=='' || $member['mb\_open'])?'checked':''; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 259 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

정보공개를 바꾸시면 앞으로 <?php echo (int)$config['cf\_open\_modify'] ?>일 이내에는 변경이 안됩니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 261 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_open\_default" value="<?php echo $member['mb\_open'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 266 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="mb\_open" value="<?php echo $member['mb\_open'] ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 269 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

정보공개는 수정후 <?php echo (int)$config['cf\_open\_modify'] ?>일 이내, <?php echo date("Y년 m월 j일", isset($member['mb\_open\_date']) ? strtotime("{$member['mb\_open\_date']} 00:00:00")+$config['cf\_open\_modify']\*86400:G5\_SERVER\_TIME+$config['cf\_open\_modify']\*86400); ?> 까지는 변경이 안됩니다.<br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 299 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="submit" id="btn\_submit" class="btn\_submit" accesskey="s"><?php echo $w==''?'회원가입':'정보수정'; ?></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 362 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

certify\_win\_open("<?php echo $cert\_type; ?>", "<?php echo $cert\_url; ?>"+params);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form\_update.tail.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$receive\_number = preg\_replace("/[^0-9]/", "", $mb\_hp);

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_form\_update.tail.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$send\_number = preg\_replace("/[^0-9]/", "", $default['de\_admin\_company\_tel']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo get\_text($mb['mb\_name']); ?></strong>님의 회원가입을 진심으로 축하합니다.

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $mb['mb\_id'] ?></strong><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\register\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $mb['mb\_email'] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['opener\_href\_wr\_id'] ?>" class="scrap\_tit" target="\_blank" onclick="opener.document.location.href='<?php echo $list[$i]['opener\_href\_wr\_id'] ?>'; return false;"><?php echo $list[$i]['subject'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['opener\_href'] ?>" class="scrap\_cate" target="\_blank" onclick="opener.document.location.href='<?php echo $list[$i]['opener\_href'] ?>'; return false;"><?php echo $list[$i]['bo\_subject'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="scrap\_datetime"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$i]['ms\_datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['del\_href']; ?>" onclick="del(this.href); return false;" class="scrap\_del"><i class="fa fa-trash-o" aria-hidden="true"></i><span class="sound\_only">삭제</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($i == 0) echo "<li class=\"empty\_li\">자료가 없습니다.</li>"; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\scrap.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($config['cf\_write\_pages'], $page, $total\_page, "?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\scrap\_popin.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\scrap\_popin.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id" value="<?php echo $wr\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\member\basic\scrap\_popin.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_text(cut\_str($write['wr\_subject'], 255)) ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $group\_select ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="mb\_id" value="<?php echo $mb\_id ?>" id="mb\_id" required class="frm\_input" size="40">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.getElementById("gr\_id").value = "<?php echo $gr\_id ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

document.getElementById("view").value = "<?php echo $view ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="view" value="<?php echo $view; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sfl" value="<?php echo $sfl; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table" value="<?php echo $bo\_table; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_bn\_id[]" value="<?php echo $i; ?>" id="chk\_bn\_id\_<?php echo $i; ?>" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_bn\_id\_<?php echo $i; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<b class="sound\_only"><?php echo $num?>번</b>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="bo\_table[<?php echo $i; ?>]" value="<?php echo $list[$i]['bo\_table']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="wr\_id[<?php echo $i; ?>]" value="<?php echo $list[$i]['wr\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_group"><a href="./new.php?gr\_id=<?php echo $list[$i]['gr\_id'] ?>"><?php echo $gr\_subject ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_board"><a href="<?php echo get\_pretty\_url($list[$i]['bo\_table']); ?>"><?php echo $bo\_subject ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 100 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><a href="<?php echo $list[$i]['href'] ?>" class="new\_tit"><?php echo $list[$i]['comment'] ?><?php echo $wr\_subject ?></a></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_name"><?php echo $list[$i]['name'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_date"><?php echo $list[$i]['datetime2'] ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<tr><td colspan="'.$colspan.'" class="empty\_table">게시물이 없습니다.</td></tr>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\new\basic\new.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\basic\outlogin.skin.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="foutlogin" action="<?php echo $outlogin\_action\_url ?>" onsubmit="return fhead\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\basic\outlogin.skin.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="url" value="<?php echo $outlogin\_url ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($member['mb\_id']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $nick ?>님</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == 'super' || $is\_auth) { ?><a href="<?php echo correct\_goto\_url(G5\_ADMIN\_URL); ?>" class="btn\_admin btn" title="관리자"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $point; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $memo\_not\_read; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="scrap"><?php echo $mb\_scrap\_cnt; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\shop\_basic\outlogin.skin.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="foutlogin" action="<?php echo $outlogin\_action\_url ?>" onsubmit="return fhead\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\shop\_basic\outlogin.skin.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="url" value="<?php echo $outlogin\_url ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="profile\_img"><?php echo get\_member\_profile\_img($member['mb\_id'], 30, 30); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="profile\_name"><?php echo $nick ?></span>님

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo G5\_BBS\_URL ?>/point.php" target="\_blank" class="win\_point">포인트<strong><?php echo $point ?></strong></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo G5\_SHOP\_URL ?>/coupon.php" target="\_blank" class="win\_coupon">쿠폰<strong><?php echo number\_format(get\_shop\_member\_coupon\_count($member['mb\_id'], true)); ?></strong></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\shop\_basic\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo G5\_BBS\_URL ?>/memo.php" target="\_blank" class="win\_memo"><span class="sound\_only">안 읽은</span>쪽지<strong><?php echo $memo\_not\_read ?></strong></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\shop\_side\outlogin.skin.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="foutlogin" action="<?php echo $outlogin\_action\_url ?>" onsubmit="return fhead\_submit(this);" method="post" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\shop\_side\outlogin.skin.1.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="url" value="<?php echo $outlogin\_url ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\shop\_side\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_member\_profile\_img($member['mb\_id']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\shop\_side\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == 'super' || $is\_auth) { ?><a href="<?php echo correct\_goto\_url(G5\_ADMIN\_URL); ?>" class="btn\_admin"><i class="fa fa-cog fa-fw"></i><span class="sound\_only">관리자</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\shop\_side\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $nick ?>님</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\shop\_side\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $point ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\shop\_side\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo number\_format($cp\_count); ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\outlogin\shop\_side\outlogin.skin.2.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $memo\_not\_read ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="po\_id" value="<?php echo $po\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == "super") { ?><a href="<?php echo G5\_ADMIN\_URL ?>/poll\_form.php?w=u&amp;po\_id=<?php echo $po\_id ?>" class="btn\_admin" title="설문관리"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">설문관리</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo $po['po\_subject'] ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="gb\_poll" value="<?php echo $i ?>" id="gb\_poll\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="gb\_poll\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $po['po\_poll'.$i] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo " alert('권한 {$po['po\_level']} 이상의 회원만 투표에 참여하실 수 있습니다.'); return false; ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo " alert('권한 {$po['po\_level']} 이상의 회원만 결과를 보실 수 있습니다.'); return false; ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_all">전체 <?php echo $nf\_total\_po\_cnt ?>표</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $po\_subject ?> 결과</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="<?php echo $poll\_1st\_class; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $list[$i]['content'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span style="width:<?php echo number\_format($list[$i]['rate'], 1) ?>%"></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="poll\_cnt"><?php echo $list[$i]['cnt'] ?> 표</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_percent"><?php echo number\_format($list[$i]['rate'], 1) ?> %</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $list2[$i]['pc\_name'] ?><span class="sound\_only">님의 의견</span></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list2[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_datetime"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list2[$i]['datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_cmt\_del"><?php if ($list2[$i]['del']) { echo $list2[$i]['del']."<i class=\"fa fa-trash-o\" aria-hidden=\"true\"></i><span class=\"sound\_only\">삭제</span></a>"; } ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list2[$i]['idea'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="po\_id" value="<?php echo $po\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_member) { ?><input type="hidden" name="pc\_name" value="<?php echo get\_text(cut\_str($member['mb\_nick'],255)) ?>"><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h3><span>기타의견</span><?php echo $po\_etc ?></h3>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_guest) { echo chk\_captcha\_js(); } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="po\_id" value="<?php echo $po\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == "super") { ?><a href="<?php echo G5\_ADMIN\_URL ?>/poll\_form.php?w=u&amp;po\_id=<?php echo $po\_id ?>" class="btn\_admin"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">설문관리</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo $po['po\_subject'] ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="gb\_poll" value="<?php echo $i ?>" id="gb\_poll\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="gb\_poll\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $po['po\_poll'.$i] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo " alert('권한 {$po['po\_level']} 이상의 회원만 투표에 참여하실 수 있습니다.'); return false; ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo " alert('권한 {$po['po\_level']} 이상의 회원만 결과를 보실 수 있습니다.'); return false; ";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h1 id="win\_title"><?php echo $g5['title'] ?></h1>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_all">전체 <?php echo $nf\_total\_po\_cnt ?>표</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $po\_subject ?> 결과</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $list[$i]['content'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span style="width:<?php echo number\_format($list[$i]['rate'], 1) ?>%"></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong class="poll\_cnt"><?php echo $list[$i]['cnt'] ?> 표</strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_percent"><?php echo number\_format($list[$i]['rate'], 1) ?> %</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $list2[$i]['pc\_name'] ?><span class="sound\_only">님의 의견</span></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 55 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list2[$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_datetime"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list2[$i]['datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="poll\_cmt\_del"><?php if ($list2[$i]['del']) { echo $list2[$i]['del']."<i class=\"fa fa-trash-o\" aria-hidden=\"true\"></i><span class=\"sound\_only\">삭제</span></a>"; } ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list2[$i]['idea'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="po\_id" value="<?php echo $po\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_member) { ?><input type="hidden" name="pc\_name" value="<?php echo get\_text(cut\_str($member['mb\_nick'],255)) ?>"><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h3><span>기타의견</span><?php echo $po\_etc ?></h3>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\poll\shop\_basic\poll\_result.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_guest) { echo chk\_captcha\_js(); } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $qaconfig['qa\_title'] ?> 카테고리</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span>Total <?php echo number\_format($total\_count) ?>건</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $page ?> 페이지

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($admin\_href) { ?><li><a href="<?php echo $admin\_href ?>" class="btn\_admin btn" title="관리자"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_qa\_sfl\_select\_options($sfl); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo stripslashes($stx); ?>" id="stx" required class="sch\_input" size="25" maxlength="15" placeholder=" 검색어를 입력해주세요">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b01 btn" title="문의등록"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">문의등록</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo get\_text($token); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<caption><?php echo $board['bo\_subject'] ?> 목록</caption>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<tr class="<?php echo $lt\_class ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 112 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="chk\_qa\_id[]" value="<?php echo $list[$i]['qa\_id'] ?>" id="chk\_qa\_id\_<?php echo $i ?>" class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="chk\_qa\_id\_<?php echo $i ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<b class="sound\_only"><?php echo $list[$i]['subject'] ?></b>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_num"><?php echo $list[$i]['num']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_cate\_link"><?php echo $list[$i]['category']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$i]['view\_href']; ?>" class="bo\_tit">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 123 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$i]['subject']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list[$i]['icon\_file']) echo " <i class=\"fa fa-download\" aria-hidden=\"true\"></i>" ; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_name"><?php echo $list[$i]['name']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_date"><?php echo $list[$i]['date']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_stat"><span class=" <?php echo ($list[$i]['qa\_status'] ? 'txt\_done' : 'txt\_rdy'); ?>"><?php echo ($list[$i]['qa\_status'] ? '답변완료' : '답변대기'); ?></span></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($i == 0) { echo '<tr><td colspan="'.$colspan.'" class="empty\_table">게시물이 없습니다.</td></tr>'; } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list\_pages; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 148 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($list\_href) { ?><li><a href="<?php echo $list\_href ?>" class="btn\_b01 btn" title="목록"><i class="fa fa-list" aria-hidden="true"></i><span class="sound\_only">목록</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 149 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\list.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b01 btn" title="문의등록"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">문의등록</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 6 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><span class="bo\_v\_reply">답변</span> <?php echo get\_text($answer['qa\_subject']); ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $answer['qa\_datetime']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $answer\_update\_href; ?>" class="btn\_b01 btn" title="답변수정">답변수정</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $answer\_delete\_href; ?>" class="btn\_b01 btn" onclick="del(this.href); return false;" title="답변삭제">답변삭제</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_view\_thumbnail(conv\_content($answer['qa\_content'], $answer['qa\_html']), $qaconfig['qa\_image\_width']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.answer.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $rewrite\_href; ?>" class="add\_qa" title="추가질문">추가질문</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qa\_id" value="<?php echo $view['qa\_id']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo $token ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_hidden;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $option; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="qa\_content\_wrap <?php echo $is\_dhtml\_editor ? $config['cf\_editor'] : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.answerform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<span class="bo\_v\_cate">'.$view['category'].'</span> ';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $view['subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성자</span><strong><?php echo $view['name'] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">작성일</span><strong class="bo\_date"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $view['datetime']; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><i class="fa fa-envelope-o" aria-hidden="true"></i> <?php echo $view['email']; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><i class="fa fa-phone" aria-hidden="true"></i> <?php echo $view['hp']; ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $list\_href ?>" class="btn\_b01 btn" title="목록"><i class="fa fa-list" aria-hidden="true"></i><span class="sound\_only">목록</span></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($write\_href) { ?><li><a href="<?php echo $write\_href ?>" class="btn\_b01 btn" title="글쓰기"><i class="fa fa-pencil" aria-hidden="true"></i><span class="sound\_only">글쓰기</span></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($update\_href) { ?><li><a href="<?php echo $update\_href ?>" class="btn\_b01 btn" title="수정">수정<i class="fa fa-pencil-square-o" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($delete\_href) { ?><li><a href="<?php echo $delete\_href ?>" class="btn\_b01 btn" onclick="del(this.href); return false;" title="삭제">삭제<i class="fa fa-trash-o" aria-hidden="true"></i></a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_view\_thumbnail($view['img\_file'][$i], $qaconfig['qa\_image\_width']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="bo\_v\_con"><?php echo get\_view\_thumbnail($view['content'], $qaconfig['qa\_image\_width']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="bo\_v\_addq"><a href="<?php echo $rewrite\_href; ?>" class="btn\_b01">추가질문</a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $view['download\_href'][$i]; ?>" class="view\_file\_download" download>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo $view['download\_source'][$i] ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 125 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($prev\_href) { ?><li><a href="<?php echo $prev\_href ?>" class="btn\_b01 btn"><i class="fa fa-chevron-left" aria-hidden="true"></i> 이전글</a></li><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($next\_href) { ?><li><a href="<?php echo $next\_href ?>" class="btn\_b01 btn">다음글 <i class="fa fa-chevron-right" aria-hidden="true"></i></a></li><?php } ?>

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($qa\_skin\_path.'/view.answer.skin.php');

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 136 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

include\_once($qa\_skin\_path.'/view.answerform.skin.php');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 159 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="bo\_cate\_link"><?php echo get\_text($rel\_list[$i]['category']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $rel\_list[$i]['view\_href']; ?>" class="bo\_tit">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 162 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $rel\_list[$i]['subject']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 165 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_date"><?php echo $rel\_list[$i]['date']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\view.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td class="td\_stat"><span class="<?php echo ($rel\_list[$i]['qa\_status'] ? 'txt\_done' : 'txt\_rdy'); ?>"><?php echo ($rel\_list[$i]['qa\_status'] ? '<i class="fa fa-check-circle" aria-hidden="true"></i> 답변완료' : '<i class="fa fa-times-circle" aria-hidden="true"></i> 답변대기'); ?></span></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fwrite" id="fwrite" action="<?php echo $action\_url ?>" onsubmit="return fwrite\_submit(this);" method="post" enctype="multipart/form-data" autocomplete="off">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qa\_id" value="<?php echo $qa\_id ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="sca" value="<?php echo $sca ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="stx" value="<?php echo $stx ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="page" value="<?php echo $page ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="token" value="<?php echo $token ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_hidden;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $category\_option ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_email" value="<?php echo get\_text($write['qa\_email']); ?>" id="qa\_email" <?php echo $req\_email; ?> class="<?php echo $req\_email.' '; ?>frm\_input full\_input email" size="50" maxlength="100" placeholder="이메일">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qa\_email\_recv" id="qa\_email\_recv" value="1" <?php if($write['qa\_email\_recv']) echo 'checked="checked"'; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_hp" value="<?php echo get\_text($write['qa\_hp']); ?>" id="qa\_hp" <?php echo $req\_hp; ?> class="<?php echo $req\_hp.' '; ?>frm\_input full\_input" size="30" placeholder="휴대폰">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qa\_sms\_recv" id="qa\_sms\_recv" value="1" <?php if($write['qa\_sms\_recv']) echo 'checked="checked"'; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qa\_subject" value="<?php echo get\_text($write['qa\_subject']); ?>" id="qa\_subject" required class="frm\_input full\_input required" size="50" maxlength="255" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="qa\_content\_wrap <?php echo $is\_dhtml\_editor ? $config['cf\_editor'] : ''; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $option; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="file" name="bf\_file[1]" id="bf\_file\_1" title="파일첨부 1 : 용량 <?php echo $upload\_max\_filesize; ?> 이하만 업로드 가능" class="frm\_file">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="bf\_file\_del1" name="bf\_file\_del[1]" value="1"> <label for="bf\_file\_del1"><?php echo $write['qa\_source1']; ?> 파일 삭제</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="file" name="bf\_file[2]" id="bf\_file\_2" title="파일첨부 2 : 용량 <?php echo $upload\_max\_filesize; ?> 이하만 업로드 가능" class="frm\_file">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" id="bf\_file\_del2" name="bf\_file\_del[2]" value="1"> <label for="bf\_file\_del2"><?php echo $write['qa\_source2']; ?> 파일 삭제</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list\_href; ?>" class="btn\_cancel btn">취소</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\qa\basic\write.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="srows" value="<?php echo $srows ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $group\_select ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<script>document.getElementById("gr\_id").value = "<?php echo $gr\_id ?>";</script>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="wr\_subject||wr\_content"<?php echo get\_selected($sfl, "wr\_subject||wr\_content") ?>>제목+내용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="wr\_subject"<?php echo get\_selected($sfl, "wr\_subject") ?>>제목</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="wr\_content"<?php echo get\_selected($sfl, "wr\_content") ?>>내용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="mb\_id"<?php echo get\_selected($sfl, "mb\_id") ?>>회원아이디</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="wr\_name"<?php echo get\_selected($sfl, "wr\_name") ?>>이름</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $text\_stx ?>" id="stx" required class="frm\_input" size="40">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 61 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" value="and" <?php echo ($sop == "and") ? "checked" : ""; ?> id="sop\_and" name="sop">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" value="or" <?php echo ($sop == "or") ? "checked" : ""; ?> id="sop\_or" name="sop" >

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><strong><?php echo $stx ?></strong> 전체검색 결과</h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li>게시판 <?php echo $board\_count ?>개</li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li>게시물 <?php echo number\_format($total\_count) ?>개</li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><?php echo number\_format($page) ?>/<?php echo number\_format($total\_page) ?> 페이지 열람 중</li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="?<?php echo $search\_query ?>&amp;gr\_id=<?php echo $gr\_id ?>" <?php echo $sch\_all ?>>전체게시판</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str\_board\_list; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 109 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><a href="<?php echo get\_pretty\_url($search\_table[$idx], '', $search\_query); ?>"><?php echo $bo\_subject[$idx] ?> 게시판 내 결과</a></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo get\_pretty\_url($search\_table[$idx], '', $search\_query); ?>" class="sch\_more">더보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$idx][$i]['href'] ?><?php echo $comment\_href ?>" class="sch\_res\_title"><?php echo $comment\_def ?><?php echo $list[$idx][$i]['subject'] ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $list[$idx][$i]['href'] ?><?php echo $comment\_href ?>" target="\_blank" class="pop\_a"><i class="fa fa-window-restore" aria-hidden="true"></i><span class="sound\_only">새창</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo $list[$idx][$i]['content'] ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $list[$idx][$i]['name'] ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 134 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sch\_datetime"><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $list[$idx][$i]['wr\_datetime'] ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 143 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\search\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $write\_pages ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxbanner.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i==0) echo '<aside id="sbn\_side" class="sbn"><h2>쇼핑몰 배너</h2><ul class="sb\_bn">'.PHP\_EOL;

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxbanner.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

echo $banner.'<img src="'.G5\_DATA\_URL.'/banner/'.$row['bn\_id'].'?'.preg\_replace('/[^0-9]/i', '', $row['bn\_time']).'" alt="'.get\_text($row['bn\_alt']).'" width="'.$size[0].'" height="'.$size[1].'"'.$bn\_border.'>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxbanner.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $banner.'<img src="'.G5\_DATA\_URL.'/banner/'.$row['bn\_id'].'?'.preg\_replace('/[^0-9]/i', '', $row['bn\_time']).'" alt="'.get\_text($row['bn\_alt']).'" width="'.$size[0].'" height="'.$size[1].'"'.$bn\_border.'>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxbanner.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i>0) echo '</ul></aside>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxcart.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="prd\_img">'.$it\_img.'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxcart.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="'.G5\_SHOP\_URL.'/cart.php" class="prd\_name">'.$it\_name.'</a>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxcart.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo number\_format($row['ct\_price']).PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxcart.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<button class="cart\_del" type="button" data-it\_id="'.$row['it\_id'].'"><i class="fa fa-trash-o" aria-hidden="true"></i><span class="sound\_only">삭제</span></button>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxcart.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="hidden" name="ct\_chk['.$i.']" value="1">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxcart.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="hidden" name="it\_id['.$i.']" value="'.$row['it\_id'].'">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxcart.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<input type="hidden" name="it\_name['.$i.']" value="'.$it\_name.'">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxcategory.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="gnb\_1dli" style="z-index:<?php echo $gnb\_zindex; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxcategory.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $row['url']; ?>" class="gnb\_1da"><?php echo $row['ca\_name']; ?><?php if ($count) echo '<i class="fa fa-angle-right" aria-hidden="true"></i>'; ?></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxcategory.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($j==0) echo '<ul class="gnb\_2dul" style="z-index:'.$gnb\_zindex.'">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxcategory.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="gnb\_2dli"><a href="<?php echo $row2['url']; ?>" class="gnb\_2da"><?php echo $row2['ca\_name']; ?></a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxcategory.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($j>0) echo '</ul>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxcommunity.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><i class="fa fa-angle-right" aria-hidden="true"></i> <a href="'.get\_pretty\_url($row['bo\_table']).'">'.$row['bo\_subject'].'</a></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="'.$href.'" class="sev\_img"><img src="'.G5\_DATA\_URL.'/event/'.$row['ev\_id'].'\_m" alt="'.$row['ev\_subject'].'"></a>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="'.$href.'" class="sev\_text">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($row['ev\_subject\_strong']) echo '<strong>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $row['ev\_subject'];

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($row['ev\_subject\_strong']) echo '</strong>';

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxevent.skin.php

The application appears to allow the use of a variable within backticks, allowing commandline execution. Carry out a manual check to determine whether the variable is user-controlled.

from `{$g5['g5\_shop\_event\_item\_table']}` a left join `{$g5['g5\_shop\_item\_table']}` b on (a.it\_id = b.it\_id)

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li class="ev\_prd\_'.$k.'">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<span class="ev\_prd\_img">'.get\_it\_image($row2['it\_id'], 110, 110, get\_text($row2['it\_name'])).'</span>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="ev\_txt\_wr"><a href="'.$item\_href.'" class="ev\_prd\_tit">'.get\_text(cut\_str($row2['it\_name'], 30)).'</a>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<span class="ev\_prd\_price">'.display\_price(get\_price($row2), $row2['it\_tel\_inq']).'</span></div>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxevent.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><a href="'.$href.'" class="sev\_more">더보기</a></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($tv\_tot\_count == 0) echo '<ul id="stv\_ul">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li class="stv\_item c'.$k.'">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $img;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo cut\_str($it\_name, 10, '').PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $print\_price.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($tv\_tot\_count > 0) echo '</ul>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 63 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var itemQty = <?php echo $tv\_tot\_count; ?>;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var itemShow = <?php echo $tv\_div['img\_length']; ?>;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var EOFlag = parseInt(<?php echo $i-1; ?>/itemShow);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxtodayview.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var itemRest = parseInt(<?php echo $i-1; ?>%itemShow);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxwish.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="prd\_img">'.$it\_img.'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxwish.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="'.shop\_item\_url($row['it\_id']).'" class="prd\_name">'.$it\_name.'</a>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\boxwish.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div class="prd\_price">'.display\_price(get\_price($item), $item['it\_tel\_inq']).'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 10 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\couponzone.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p><?php echo $default['de\_admin\_company\_name']; ?> 회원이시라면 쿠폰 다운로드 후 바로 사용하실 수 있습니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\couponzone.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<ul>'.PHP\_EOL.$coupon.'</ul>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\couponzone.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p>보유하신 <?php echo $default['de\_admin\_company\_name']; ?> 회원 포인트를 쿠폰으로 교환하실 수 있습니다.</p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 187 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\couponzone.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<ul>'.PHP\_EOL.$coupon.'</ul>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 8 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form name="fitem" method="post" action="<?php echo $action\_url; ?>" onsubmit="return fitem\_submit(this);">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id[]" value="<?php echo $it\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="'.G5\_SHOP\_URL.'/largeimage.php?it\_id='.$it['it\_id'].'&amp;no='.$i.'" target="\_blank" class="popup\_item\_image">'.$img.'</a>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo G5\_SHOP\_URL; ?>/largeimage.php?it\_id=<?php echo $it['it\_id']; ?>&amp;no=1" target="\_blank" id="popup\_item\_image" class="popup\_item\_image"><i class="fa fa-search-plus" aria-hidden="true"></i><span class="sound\_only">확대보기</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li '.$sit\_pvi\_last.'>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<a href="'.G5\_SHOP\_URL.'/largeimage.php?it\_id='.$it['it\_id'].'&amp;no='.$thumb\_count.'" target="\_blank" class="popup\_item\_image img\_thumb">'.$val.'<span class="sound\_only"> '.$thumb\_count.'번째 이미지 새창</span></a>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 id="sit\_title"><?php echo stripslashes($it['it\_name']); ?> <span class="sound\_only">요약정보 및 구매</span></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<p id="sit\_desc"><?php echo $it['it\_basic']; ?></p>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

상품 선택옵션 <?php echo $option\_count; ?> 개, 추가옵션 <?php echo $supply\_count; ?> 개

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<img src="<?php echo G5\_SHOP\_URL; ?>/img/s\_star<?php echo $star\_score?>.png" alt="" class="sit\_star" width="100">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">별<?php echo $star\_score?>개</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="">사용후기 <?php echo $it['it\_use\_cnt']; ?> 개</span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span id="btn\_wish"><i class="fa fa-heart-o" aria-hidden="true"></i><span class="sound\_only">위시리스트</span><span class="btn\_wish\_num"><?php echo get\_wishlist\_count\_by\_item($it['it\_id']); ?></span></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $sns\_share\_links; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:popup\_item\_recommend('<?php echo $it['it\_id']; ?>');" id="sit\_btn\_rec"><i class="fa fa-envelope-o" aria-hidden="true"></i><span class="sound\_only">추천하기</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 124 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo display\_price($it['it\_cust\_price']); ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<strong><?php echo display\_price(get\_price($it)); ?></strong>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" id="it\_price" value="<?php echo get\_price($it); ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $it['it\_maker']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $it['it\_origin']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 154 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $it['it\_brand']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 161 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $it['it\_model']; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 180 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '구매금액(추가옵션 제외)의 '.$it['it\_point'].'%';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 183 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo number\_format($it\_point).'점';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 209 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th><?php echo $ct\_send\_cost\_label; ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 210 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $sc\_method; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 215 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($it['it\_buy\_min\_qty']); ?> 개</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 221 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo number\_format($it['it\_buy\_max\_qty']); ?> 개</td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 235 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $option\_item;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 250 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $supply\_item;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 269 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_type[<?php echo $it\_id; ?>][]" value="0">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 270 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_id[<?php echo $it\_id; ?>][]" value="">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 271 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="io\_value[<?php echo $it\_id; ?>][]" value="<?php echo $it['it\_name']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 273 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" class="io\_stock" value="<?php echo $it['it\_stock\_qty']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 275 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sit\_opt\_subj"><?php echo $it['it\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 278 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ct\_qty\_<?php echo $i; ?>" class="sound\_only">수량</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 280 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ct\_qty[<?php echo $it\_id; ?>][]" value="<?php echo $it['it\_buy\_min\_qty']; ?>" id="ct\_qty\_<?php echo $i; ?>" class="num\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 308 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:item\_wish(document.fitem, '<?php echo $it['it\_id']; ?>');" class="sit\_btn\_wish"><i class="fa fa-heart-o" aria-hidden="true"></i><span class="sound\_only">위시리스트</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 311 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="javascript:popup\_stocksms('<?php echo $it['it\_id']; ?>');" id="sit\_btn\_alm">재입고알림</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 314 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="itemform-naverpay"><?php echo $naverpay\_request\_js.$naverpay\_button\_js; ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 358 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $prev\_href.$prev\_title.$prev\_href2;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 359 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $next\_href.$next\_title.$next\_href2;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 408 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var min\_qty = parseInt(<?php echo $it['it\_buy\_min\_qty']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 409 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var max\_qty = parseInt(<?php echo $it['it\_buy\_max\_qty']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 458 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

f.action = "<?php echo $action\_url; ?>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 480 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var min\_qty = parseInt(<?php echo $it['it\_buy\_min\_qty']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 481 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.form.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

var max\_qty = parseInt(<?php echo $it['it\_buy\_max\_qty']; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><button type="button" id="btn\_sit\_use" rel="#sit\_use">사용후기 <span class="item\_use\_count"><?php echo $item\_use\_count; ?></span></button></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><button type="button" id="btn\_sit\_qa" rel="#sit\_qa">상품문의 <span class="item\_qa\_count"><?php echo $item\_qa\_count; ?></span></button></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($it['it\_explan'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<th scope="row"><?php echo $ii\_title; ?></th>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<td><?php echo $ii\_value; ?></td>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($default['de\_baesong\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo conv\_content($default['de\_change\_content'], 1); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 141 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo str\_replace(array('class="get\_item\_options"', 'id="it\_option\_', 'class="it\_option"'), array('class="get\_side\_item\_options"', 'id="it\_side\_option\_', 'class="it\_side\_option"'), $option\_item);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo str\_replace(array('id="it\_supply\_', 'class="it\_supply"'), array('id="it\_side\_supply\_', 'class="it\_side\_supply"'), $supply\_item);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 166 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sit\_opt\_subj"><?php echo $it['it\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 169 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<label for="ct\_qty\_<?php echo $i; ?>" class="sound\_only">수량</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 171 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\item.info.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="ct\_copy\_qty[<?php echo $it\_id; ?>][]" value="<?php echo $it['it\_buy\_min\_qty']; ?>" id="ct\_qty\_<?php echo $i; ?>" class="num\_input" size="5">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemqa\_form; ?>" class="btn02 itemqa\_form">상품문의 쓰기<span class="sound\_only">새 창</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemqa\_list; ?>" id="itemqa\_list" class="btn01">더보기</a>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqa.skin.php

MD5 Hashing algorithm.

$hash = md5($row['iq\_id'].$row['iq\_time'].$row['iq\_ip']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<ol id="sit\_qa\_ol">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button type="button" class="sit\_qa\_li\_title"><span class="<?php echo $iq\_style; ?>"><?php echo $iq\_stats; ?></span><?php echo $iq\_subject; ?></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo $iq\_name; ?><span class="st\_bg"></span><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $iq\_time; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sit\_qa\_con\_<?php echo $i; ?>" class="sit\_qa\_con">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $iq\_question;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $iq\_answer; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemqa\_form."&amp;iq\_id={$row['iq\_id']}&amp;w=u"; ?>" class="itemqa\_form btn01" onclick="return false;">수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemqa\_formupdate."&amp;iq\_id={$row['iq\_id']}&amp;w=d&amp;hash={$hash}"; ?>" class="itemqa\_delete btn01">삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo '</ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (!$i) echo '<p class="sit\_empty">상품문의가 없습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqa.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo itemqa\_page($config['cf\_write\_pages'], $page, $total\_page, G5\_SHOP\_URL."/itemqa.php?it\_id=$it\_id&amp;page=", "");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id" value="<?php echo $it\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="iq\_id" value="<?php echo $iq\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="iq\_secret" id="iq\_secret" value="1" <?php echo $chk\_secret; ?> class="selec\_chk">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="iq\_email" id="iq\_email" value="<?php echo get\_text($qa['iq\_email']); ?>" class="frm\_input full\_input" size="30" placeholder="이메일"><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="iq\_hp" id="iq\_hp" value="<?php echo get\_text($qa['iq\_hp']); ?>" class="frm\_input full\_input" size="20" placeholder="휴대폰"><br>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="iq\_subject" value="<?php echo get\_text($qa['iq\_subject']); ?>" id="iq\_subject" required class="required frm\_input" maxlength="250" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqaform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 12 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form method="get" action="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="b.it\_name" <?php echo get\_selected($sfl, "b.it\_name", true); ?>>상품명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.it\_id" <?php echo get\_selected($sfl, "a.it\_id"); ?>>상품코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.iq\_subject" <?php echo get\_selected($sfl, "a.iq\_subject"); ?>>문의제목</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.iq\_question"<?php echo get\_selected($sfl, "a.iq\_question"); ?>>문의내용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.iq\_name" <?php echo get\_selected($sfl, "a.iq\_name"); ?>>작성자명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 22 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.mb\_id" <?php echo get\_selected($sfl, "a.mb\_id"); ?>>작성자아이디</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx; ?>" id="stx" required class="sch\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">전체보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <p><?php echo $config['cf\_title']; ?> 전체 상품문의 목록입니다.</p> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $it\_href; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 77 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_it\_image($row['it\_id'], 50, 50); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $row['it\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 83 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><?php echo $iq\_subject; ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="<?php echo $iq\_style; ?>"><?php echo $iq\_stats; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><i class="fa fa-user" aria-hidden="true"></i> <?php echo $row['iq\_name']; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo substr($row['iq\_time'],0,10); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sqa\_con\_<?php echo $i; ?>" class="sqa\_con" style="display:none;">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $iq\_question;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $iq\_answer; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sqa\_con\_btn"><button class="sqa\_con\_<?php echo $i; ?>">내용보기 <i class="fa fa-caret-down" aria-hidden="true"></i></button></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 116 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo '</ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<p id="sqa\_empty">자료가 없습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemqalist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h4>구매고객 총평점 <span>(총 <strong><?php echo $total\_count; ?></strong> 건 상품평 기준)</span></h4>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<img src="<?php echo G5\_SHOP\_URL; ?>/img/s\_star<?php echo $star\_score?>.png" alt="" class="sit\_star">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemuse\_form; ?>" class="btn02 itemuse\_form">사용후기 쓰기<span class="sound\_only"> 새 창</span></a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemuse\_list; ?>" class="btn01 itemuse\_list">더보기</a>

**MEDIUM: Potentially Unsafe Code - md5**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

MD5 Hashing algorithm.

$hash = md5($row['is\_id'].$row['is\_time'].$row['is\_ip']);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<ol id="sit\_use\_ol">';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sit\_thum"><?php echo get\_itemuselist\_thumbnail($row['it\_id'], $row['is\_content'], 100, 100); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sit\_use\_star"><img src="<?php echo G5\_SHOP\_URL; ?>/img/s\_star<?php echo $is\_star; ?>.png" alt="별<?php echo $is\_star; ?>개" width="85"></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd class="sit\_use\_tit"><?php echo $is\_subject; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><?php echo $is\_name; ?><span class="st\_bg"></span><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $is\_time; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sit\_use\_con\_<?php echo $i; ?>" class="sit\_use\_con">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemuse\_form."&amp;is\_id={$row['is\_id']}&amp;w=u"; ?>" class="itemuse\_form btn01" onclick="return false;">수정</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $itemuse\_formupdate."&amp;is\_id={$row['is\_id']}&amp;w=d&amp;hash={$hash}"; ?>" class="itemuse\_delete btn01">삭제</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_reply\_subject;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_reply\_name;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 79 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_reply\_content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo '</ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if (!$i) echo '<p class="sit\_empty">사용후기가 없습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuse.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo itemuse\_page($config['cf\_write\_pages'], $page, $total\_page, G5\_SHOP\_URL."/itemuse.php?it\_id=$it\_id&amp;page=", "");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="w" value="<?php echo $w; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="it\_id" value="<?php echo $it\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="is\_id" value="<?php echo $is\_id; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="is\_subject" value="<?php echo get\_text($use['is\_subject']); ?>" id="is\_subject" required class="required frm\_input full\_input" maxlength="250" placeholder="제목">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_html; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="5" id="is\_score5" <?php echo ($is\_score==5)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="4" id="is\_score4" <?php echo ($is\_score==4)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="3" id="is\_score3" <?php echo ($is\_score==3)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="2" id="is\_score2" <?php echo ($is\_score==2)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="radio" name="is\_score" value="1" id="is\_score1" <?php echo ($is\_score==1)?'checked="checked"':''; ?>>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuseform.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $editor\_js; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 11 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<form method="get" action="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="b.it\_name" <?php echo get\_selected($sfl, "b.it\_name"); ?>>상품명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.it\_id" <?php echo get\_selected($sfl, "a.it\_id"); ?>>상품코드</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 18 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.is\_subject"<?php echo get\_selected($sfl, "a.is\_subject"); ?>>후기제목</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.is\_content"<?php echo get\_selected($sfl, "a.is\_content"); ?>>후기내용</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.is\_name" <?php echo get\_selected($sfl, "a.is\_name"); ?>>작성자명</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="a.mb\_id" <?php echo get\_selected($sfl, "a.mb\_id"); ?>>작성자아이디</option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="stx" value="<?php echo $stx; ?>" id="stx" required class="sch\_input">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $\_SERVER['SCRIPT\_NAME']; ?>">전체보기</a>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<!-- <p><?php echo $config['cf\_title']; ?> 전체 사용후기 목록입니다.</p> -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<a href="<?php echo $it\_href; ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_it\_image($row['it\_id'], 100, 100); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo $row2['it\_name']; ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button class="prd\_detail" data-url="<?php echo G5\_SHOP\_URL.'/largeimage.php?it\_id='.$row['it\_id']; ?>"><i class="fa fa-camera" aria-hidden="true"></i><span class="sound\_only">상품 이미지보기</span></button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><img src="<?php echo G5\_URL; ?>/shop/img/s\_star<?php echo $star; ?>.png" alt="별<?php echo $star; ?>개" width="80"></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sps\_pd\_name"><?php echo get\_text($row2['it\_name']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 65 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sps\_rv\_tit"><?php echo get\_text($row['is\_subject']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sps\_rv\_thum"><?php echo get\_itemuse\_thumb($row['is\_content'], 60, 60); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><i class="fa fa-user" aria-hidden="true"></i> <?php echo $row['is\_name']; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo substr($row['is\_time'],0,10); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<button class="sps\_con\_<?php echo $i; ?> review\_detail">내용보기</button>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo get\_text($row['is\_subject']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><i class="fa fa-user" aria-hidden="true"></i> <?php echo $row['is\_name']; ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 89 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo substr($row['is\_time'],0,10); ?></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_it\_image($row['it\_id'], 50, 50); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span><?php echo get\_text($row2['it\_name']); ?></span>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<span class="sound\_only">평가점수</span><img src="<?php echo G5\_URL; ?>/shop/img/s\_star<?php echo $star; ?>.png" alt="별<?php echo $star; ?>개" width="80">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sps\_con\_<?php echo $i; ?>" class="review\_bt\_cnt">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2 class="is\_use\_reply"><?php echo get\_text($row['is\_reply\_subject']); ?></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<i class="fa fa-clock-o" aria-hidden="true"></i> <?php echo $row['is\_reply\_name']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sps\_con\_<?php echo $i; ?>\_reply">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $is\_reply\_content;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 0) echo '</ol>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i == 0) echo '<p id="sps\_empty">자료가 없습니다.</p>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\itemuselist.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_paging($config['cf\_write\_pages'], $page, $total\_page, "{$\_SERVER['SCRIPT\_NAME']}?$qstr&amp;page="); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 20 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\largeimage.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $imgs['imagehtml']; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\largeimage.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><a href="'.G5\_SHOP\_URL.'/largeimage.php?it\_id='.$it\_id.'&amp;no='.$key.'" class="img\_thumb">'.$val.'</a></li>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\largeimage.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$("#sit\_pvi\_nwbig span:eq("+<?php echo ($no - 1); ?>+")").addClass("visible");

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\largeimage.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

largeimage\_load(<?php echo $size[0]; ?>);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li ".implode(' ', $classes)."\" data-css=\"nocss\" style=\"height:auto\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_star\"><span class=\"sound\_only\">고객평점</span><img src=\"".G5\_SHOP\_URL."/img/s\_star".$star\_score.".png\" alt=\"별점 ".$star\_score."점\" class=\"sit\_star\"></div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_basic\">".stripslashes($row['it\_basic'])."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 110 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<span class=\"sct\_dict\">".display\_price($row['it\_cust\_price'])."</span>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<button type=\"button\" class=\"btn\_wish\" data-it\_id=\"{$row['it\_id']}\"><span class=\"sound\_only\">위시리스트</span><i class=\"fa fa-heart-o\" aria-hidden=\"true\"></i></button>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 129 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/facebook.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 130 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/twitter.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 131 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/gplus.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 142 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sit\_icon\_li\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 150 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i >= 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 152 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i === 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$sct\_last}\" data-css=\"nocss\" style=\"width:{$this->img\_width}px\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_icon\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_basic\">".stripslashes($row['it\_basic'])."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<span class=\"sct\_dict\">".display\_price($row['it\_cust\_price'])."</span>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 93 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/sns\_fb\_s.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/sns\_twt\_s.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 95 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/sns\_goo\_s.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i >= 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$sct\_last}\" data-css=\"nocss\" style=\"padding:{$list\_top\_pad}px {$list\_right\_pad}px {$list\_bottom\_pad}px {$list\_left\_pad}px;width:{$list\_width}px;height:{$list\_height}px\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 46 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 50 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_icon\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 66 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_basic\">".stripslashes($row['it\_basic'])."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<span class=\"sct\_dict\">".display\_price($row['it\_cust\_price'])."</span>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 90 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 101 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/sns\_fb\_s.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/sns\_twt\_s.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/sns\_goo\_s.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 108 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_arw\_toleft\" style=\"left:{$arrow\_left}px\"></div>";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 113 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i >= 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 115 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$sct\_last}\" data-css=\"nocss\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 60 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_icon\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_basic\">".stripslashes($row['it\_basic'])."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<span class=\"sct\_dict\">".display\_price($row['it\_cust\_price'])."</span>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<button type=\"button\" class=\"btn\_wish\" data-it\_id=\"{$row['it\_id']}\"><span class=\"sound\_only\">위시리스트</span><i class=\"fa fa-heart-o\" aria-hidden=\"true\"></i></button>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 117 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/facebook.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 118 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/twitter.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/gplus.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_rel\">".relation\_item($row['it\_id'], 70, 0, 5)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 133 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i >= 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_name&amp;sortodr=asc">상품명순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_type1&amp;sortodr=desc">히트상품</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_type2&amp;sortodr=desc">추천상품</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_type3&amp;sortodr=desc">최신상품</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_type4&amp;sortodr=desc">인기상품</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_type5&amp;sortodr=desc">할인상품</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_sum\_qty&amp;sortodr=desc">판매많은순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_price&amp;sortodr=asc">낮은가격순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_price&amp;sortodr=desc">높은가격순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 40 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_use\_avg&amp;sortodr=desc">평점높은순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_use\_cnt&amp;sortodr=desc">후기많은순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 42 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\list.sort.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li><a href="<?php echo $sct\_sort\_href; ?>it\_update\_time&amp;sortodr=desc">최근등록순</a></li>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\listcategory.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\listcategory2.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\listcategory3.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo $str; ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"sct smt\_40 owl-carousel\" data-value=\"".$this->list\_mod."\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li {$sct\_last}\" style=\"width:{$this->img\_width}px\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 41 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 67 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_star\"><span class=\"sound\_only\">고객평점</span><img src=\"".G5\_SHOP\_URL."/img/s\_star".$star\_score.".png\" alt=\"별점 ".$star\_score."점\" class=\"sit\_star\"></div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 71 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 75 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 97 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i >= 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<ul id="btn\_smt\_<?php echo $this->type; ?>" class="sctrl">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div id=\"smt\_{$this->type}\" class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 39 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div id=\"smt\_{$this->type}\" class=\"sct smt\_20\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$sct\_last}\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 52 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 68 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_basic\">".stripslashes($row['it\_basic'])."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 88 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<span class=\"sct\_dict\">".display\_price($row['it\_cust\_price'])."</span>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 103 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_sns\" style=\"top:{$sns\_top}px\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 104 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/facebook.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 105 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/twitter.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/gplus.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 111 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_icon\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 122 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 254 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$("#smt\_<?php echo $this->type; ?>").topRolling();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 259 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$("#btn\_smt\_<?php echo $this->type; ?> button.sctrl\_play").on("click", function() {

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 260 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$("#btn\_smt\_<?php echo $this->type; ?> button.sctrl\_stop").data("stop", false);

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 268 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.20.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

$("#btn\_smt\_<?php echo $this->type; ?> button.sctrl\_stop").on("click", function() {

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$sct\_last}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<span class="sct\_disc">'.$sale\_per.'</span>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 74 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_star\"><span class=\"sound\_only\">고객평점</span><img src=\"".G5\_SHOP\_URL."/img/s\_star".$star\_score.".png\" alt=\"별점 ".$star\_score."점\" class=\"sit\_star\"></div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 78 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 82 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_basic\">".stripslashes($row['it\_basic'])."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 102 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<span class=\"sct\_dict\">".display\_price($row['it\_cust\_price'])."</span>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 106 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 114 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<button type=\"button\" class=\"btn\_wish\" data-it\_id=\"{$row['it\_id']}\"><span class=\"sound\_only\">위시리스트</span><i class=\"fa fa-heart-o\" aria-hidden=\"true\"></i></button>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 126 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/facebook.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 127 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/twitter.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 128 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/gplus.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 139 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sit\_icon\_li\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 145 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i >= 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 147 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.30.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 38 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li{$sct\_last}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_star\"><span class=\"sound\_only\">고객평점</span><img src=\"".G5\_SHOP\_URL."/img/s\_star".$star\_score.".png\" alt=\"별점 ".$star\_score."점\" class=\"sit\_star\"></div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 76 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 80 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 92 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_basic\">".stripslashes($row['it\_basic'])."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 99 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 107 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<button type=\"button\" class=\"btn\_wish\" data-it\_id=\"{$row['it\_id']}\"><span class=\"sound\_only\">위시리스트</span><i class=\"fa fa-heart-o\" aria-hidden=\"true\"></i></button>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 119 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/facebook.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 120 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/twitter.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 121 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/gplus.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 132 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sit\_icon\_li\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 138 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i >= 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 140 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.40.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul id=\"smt\_{$this->type}\" class=\"smt\_30\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li sct\_li\_{$i}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<span class=\"sound\_only\">고객평점</span><img src=\"".G5\_SHOP\_URL."/img/s\_star".$star\_score.".png\" alt=\"별 ".$star\_score."개\" class=\"sit\_star\" width=\"100\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 48 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<span class=\"sct\_dict\">".display\_price($row['it\_cust\_price'])."</span>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 62 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i >= 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 70 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\main.50.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 0) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\mainbanner.10.skin.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

$item\_html .= $banner.'<img src="'.G5\_DATA\_URL.'/banner/'.$row['bn\_id'].'?'.preg\_replace('/[^0-9]/i', '', $row['bn\_time']).'" width="'.$size[0].'" alt="'.get\_text($row['bn\_alt']).'"'.$bn\_border.'>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 54 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\mainbanner.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i==0) echo '<div id="main\_bn"><div class="main\_image\_area"><div class="main\_banner\_owl owl-carousel">'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 56 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\mainbanner.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $item\_html;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 72 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\mainbanner.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li class="owl-dot"><a data-slide-index="'.$k.'" href="#">'.$alt\_title.'</a></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\navigation.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div id="sct\_location" class="<?php echo implode(' ', $location\_class);?>"> <!-- class="view\_location" --> <!-- view\_location는 리스트 말고 상품보기에서만 표시 -->

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 43 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\navigation.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $data['ca\_id']; ?>" data-url="<?php echo $data['url']; ?>" <?php if($ca\_ids['ca\_id'] === $data['ca\_id']) echo 'selected'; ?>><?php echo $data['ca\_name']; ?></option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 51 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\navigation.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $data['ca\_id']; ?>" data-url="<?php echo $data['url']; ?>" <?php if($ca\_ids['ca\_id2'] === $data['ca\_id']) echo 'selected'; ?>><?php echo $data['ca\_name']; ?></option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 59 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\navigation.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<option value="<?php echo $data['ca\_id']; ?>" data-url="<?php echo $data['url']; ?>" <?php if($ca\_ids['ca\_id3'] === $data['ca\_id']) echo 'selected'; ?>><?php echo $data['ca\_name']; ?></option>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\navigation.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php echo get\_text($g5['title']); ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<li class="sct\_li<?php echo $sct\_last; ?>" style="width:<?php echo $img\_width; ?>px">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 25 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sct\_img"><a href="<?php echo $href; ?>" class="sct\_a"><img src="<?php echo G5\_SHOP\_SKIN\_URL; ?>/img/personal.jpg" alt=""></a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 26 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sct\_txt"><a href="<?php echo $href; ?>" class="sct\_a"><?php echo get\_text($row['pp\_name']).'님 개인결제'; ?></a></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<div class="sct\_cost"><?php echo display\_price($row['pp\_price']); ?></div>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 34 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\personalpay.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 1) echo "<p class=\"sct\_noitem\">등록된 개인결제가 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 24 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<ul class=\"{$this->css}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li class=\"sct\_li slide {$sct\_last}\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 33 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_img\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_it\_image($row['it\_id'], $this->img\_width, $this->img\_height, '', '', stripslashes($row['it\_name']))."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_icon\">".item\_icon($row)."</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_id\">&lt;".stripslashes($row['it\_id'])."&gt;</div>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 53 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_txt\"><a href=\"{$item\_link\_href}\" class=\"sct\_a\">\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 57 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo stripslashes($row['it\_name'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 69 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<strike>".display\_price($row['it\_cust\_price'])."</strike>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 73 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo display\_price(get\_price($row), $row['it\_tel\_inq'])."\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 84 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<div class=\"sct\_sns\" style=\"top:{$sns\_top}px\">";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 85 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('facebook', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/sns\_fb\_s.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 86 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('twitter', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/sns\_twt\_s.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 87 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_sns\_share\_link('googleplus', $sns\_url, $sns\_title, G5\_SHOP\_SKIN\_URL.'/img/sns\_goo\_s.png');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if ($i > 1) echo "</ul>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 96 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\relation.10.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

if($i == 1) echo "<p class=\"sct\_noitem\">등록된 상품이 없습니다.</p>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 9 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<h2><strong><?php echo $q; ?></strong> 검색 결과<span class="ssch\_result\_total">총 <?php echo $total\_count; ?>건</span></h2>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 14 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qsort" id="qsort" value="<?php echo $qsort ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qorder" id="qorder" value="<?php echo $qorder ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 16 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="hidden" name="qcaid" id="qcaid" value="<?php echo $qcaid ?>">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="q" value="<?php echo $q; ?>" id="ssch\_q" class="ssch\_input" size="40" maxlength="30" placeholder="검색어">

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qname" id="ssch\_qname" value="1" <?php echo $qname\_check?'checked="checked"':'';?>> <label for="ssch\_qname"><span></span>상품명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 30 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qexplan" id="ssch\_qexplan" value="1" <?php echo $qexplan\_check?'checked="checked"':'';?>> <label for="ssch\_qexplan"><span></span>상품설명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 31 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qbasic" id="ssch\_qbasic" value="1" <?php echo $qbasic\_check?'checked="checked"':'';?>> <label for="ssch\_qbasic"><span></span>기본설명</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 32 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="checkbox" name="qid" id="ssch\_qid" value="1" <?php echo $qid\_check?'checked="checked"':'';?>> <label for="ssch\_qid"><span></span>상품코드</label>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qfrom" value="<?php echo $qfrom; ?>" id="ssch\_qfrom" class="ssch\_input" size="10"> 원 ~

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 37 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<input type="text" name="qto" value="<?php echo $qto; ?>" id="ssch\_qto" class="ssch\_input" size="10"> 원

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 45 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<li><a href="#" onclick="set\_ca\_id(\'\'); return false;">전체분류 <span>('.$total\_count.')</span></a></li>'.PHP\_EOL;

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 49 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "<li><a href=\"#\" onclick=\"set\_ca\_id('{$row['ca\_id']}'); return false;\">{$row['ca\_name']} (".$row['cnt'].")</a></li>\n";

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 81 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo $list->run();

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 91 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo '<div>'.$error.'</div>';

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 98 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\shop\basic\search.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo get\_paging($config['cf\_write\_pages'], $page, $total\_page, $\_SERVER['SCRIPT\_NAME'].'?'.$query\_string.'&amp;page=');

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><strong><?php echo number\_format($visit[1]) ?></strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><strong><?php echo number\_format($visit[2]) ?></strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><strong><?php echo number\_format($visit[3]) ?></strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><strong><?php echo number\_format($visit[4]) ?></strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\visit\basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == "super") { ?><a href="<?php echo G5\_ADMIN\_URL ?>/visit\_list.php" class="btn\_admin btn"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a><?php } ?>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 15 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\visit\shop\_basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><strong><?php echo number\_format($visit[1]) ?></strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\visit\shop\_basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><strong><?php echo number\_format($visit[2]) ?></strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\visit\shop\_basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><strong><?php echo number\_format($visit[3]) ?></strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 21 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\visit\shop\_basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<dd><strong><?php echo number\_format($visit[4]) ?></strong></dd>

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 23 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2022 1252\Buggy\gnuboard5-5.5.5\gnuboard5-5.5.5\theme\basic\skin\visit\shop\_basic\visit.skin.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

<?php if ($is\_admin == "super") { ?><a href="<?php echo G5\_ADMIN\_URL ?>/visit\_list.php" class="btn\_admin btn"><i class="fa fa-cog fa-spin fa-fw"></i><span class="sound\_only">관리자</span></a><?php } ?>