그누보드
XSS 취약점

소프트웨어공학부 정보보호학전공

91913531 서민재

목차

XSS

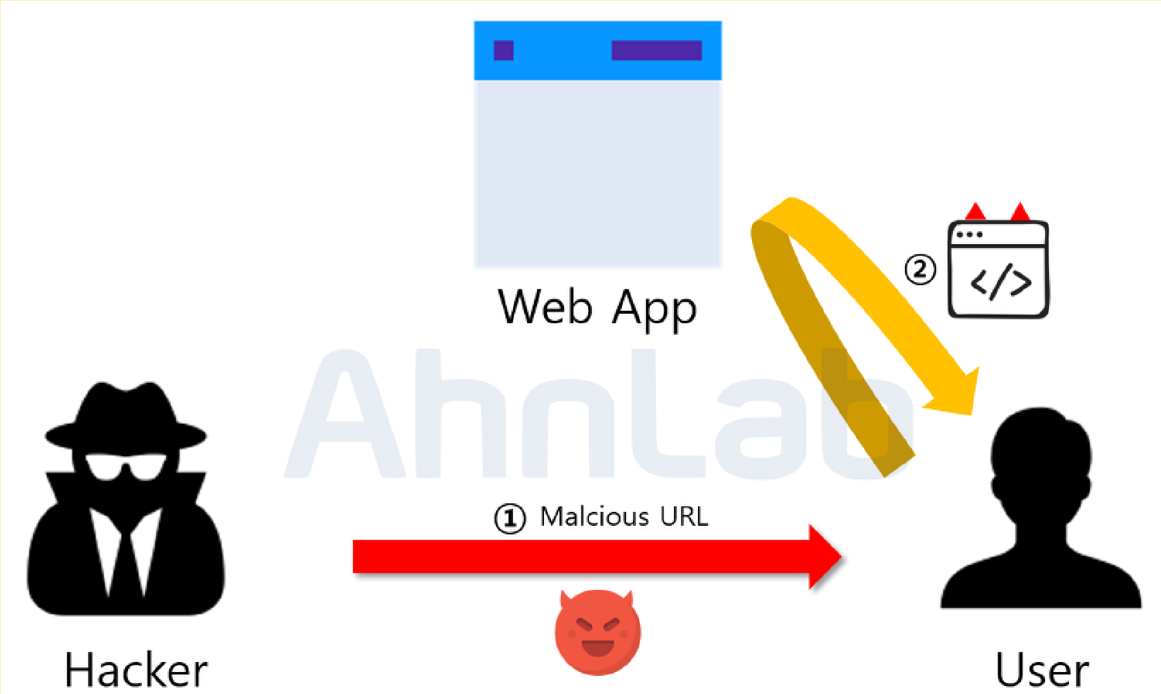
그누보드

개요

[KVE-2020-1616]
그누보드 메인화면 XSS 취약점

XSS

XSS

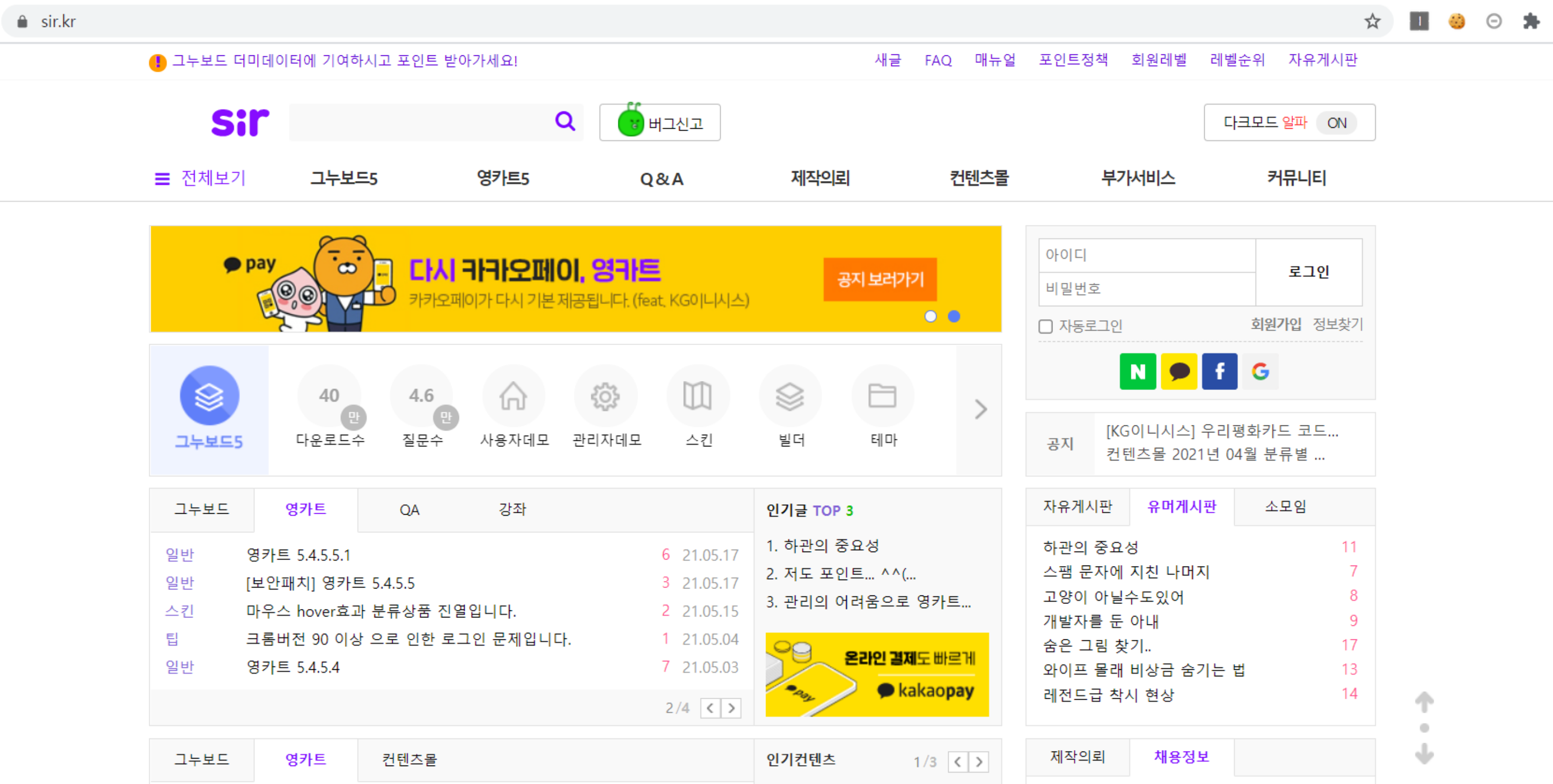


악의적인 사용자가 공격하려는 사이트에 스크립트를 넣는 기법

사용자의 정보(쿠키, 세션, 토큰 등) 탈취

그누보드

그누보드란?



그누보드 더미데이터에 기여하시고 포인트 받아가세요!

공지 [KG이니시스] 우리평화카드 코드...
컨텐츠몰 2021년 04월 분류별 ...

일반	영카트 5.4.5.5.1	6	21.05.17
일반	[보안패치] 영카트 5.4.5.5	3	21.05.17
스킨	마우스 hover효과 분류상품 진열입니다.	2	21.05.15
팁	크롬버전 90 이상 으로 인한 로그인 문제입니다.	1	21.05.04
일반	영카트 5.4.5.4	7	21.05.03

1. 하관의 중요성
2. 저도 포인트... ^^(...
3. 관리의 어려움으로 영카트...

하관의 중요성	11
스팸 문자에 지친 나머지	7
고양이 아닐수도있어	8
개발자를 둔 아내	9
숨은 그림 찾기..	17
와이프 몰래 비상금 숨기는 법	13
레전드급 착시 현상	14

PHP 기반 오픈소스 설치형 인터넷 게시판 프로그램

그누보드란?

CMS

(Contents Management System)

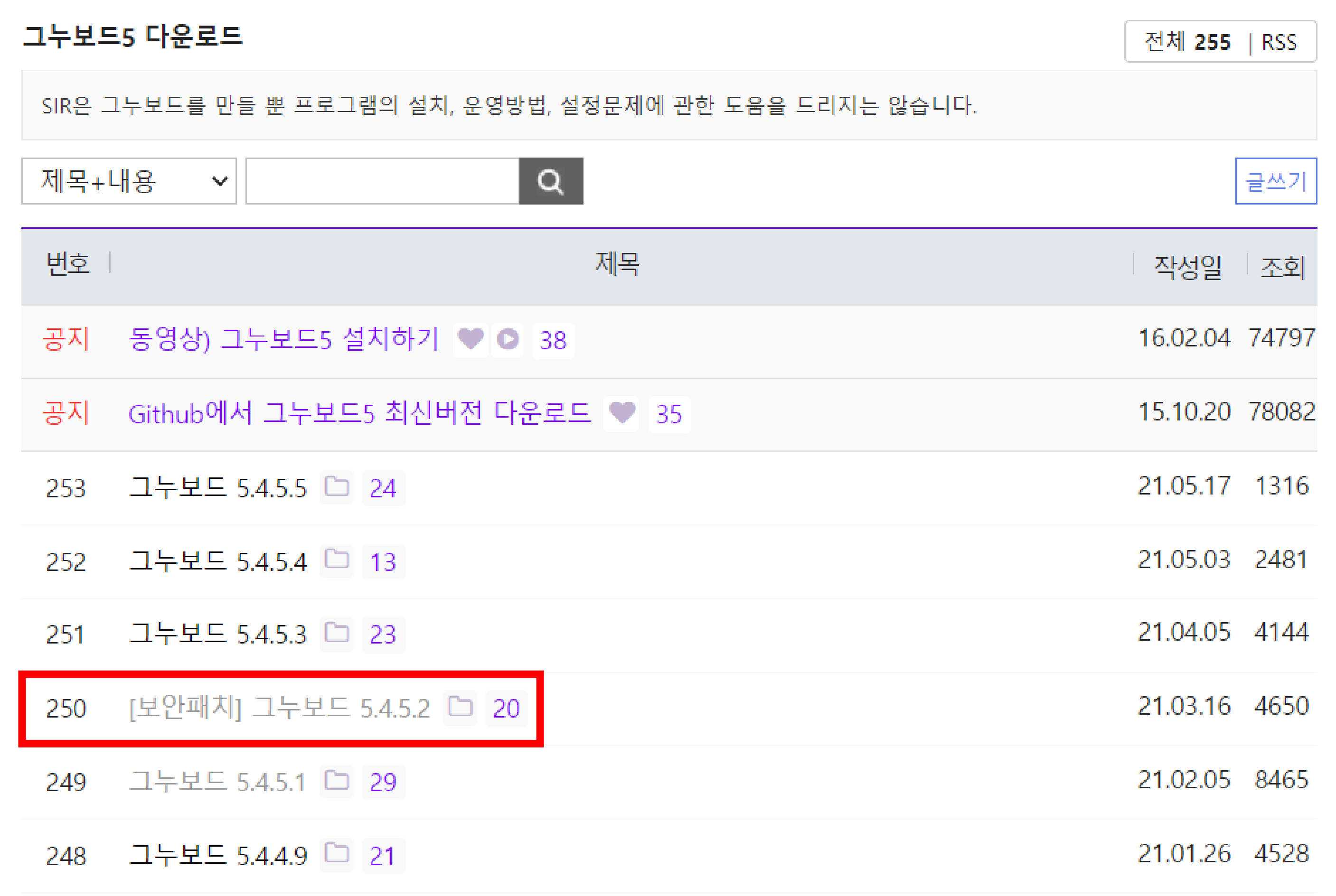
게시판, 레이아웃, 모듈과 같은 기능을 모아둔 웹 프레임워크

기본적인 작업 자동화
-> 웹 사이트 제작에 드는 시간 감소, 개발속도 빨라짐

프레임워크 단위의 도구 제공
-> 새로운 기능 간단하게 구현 가능

개요

개요



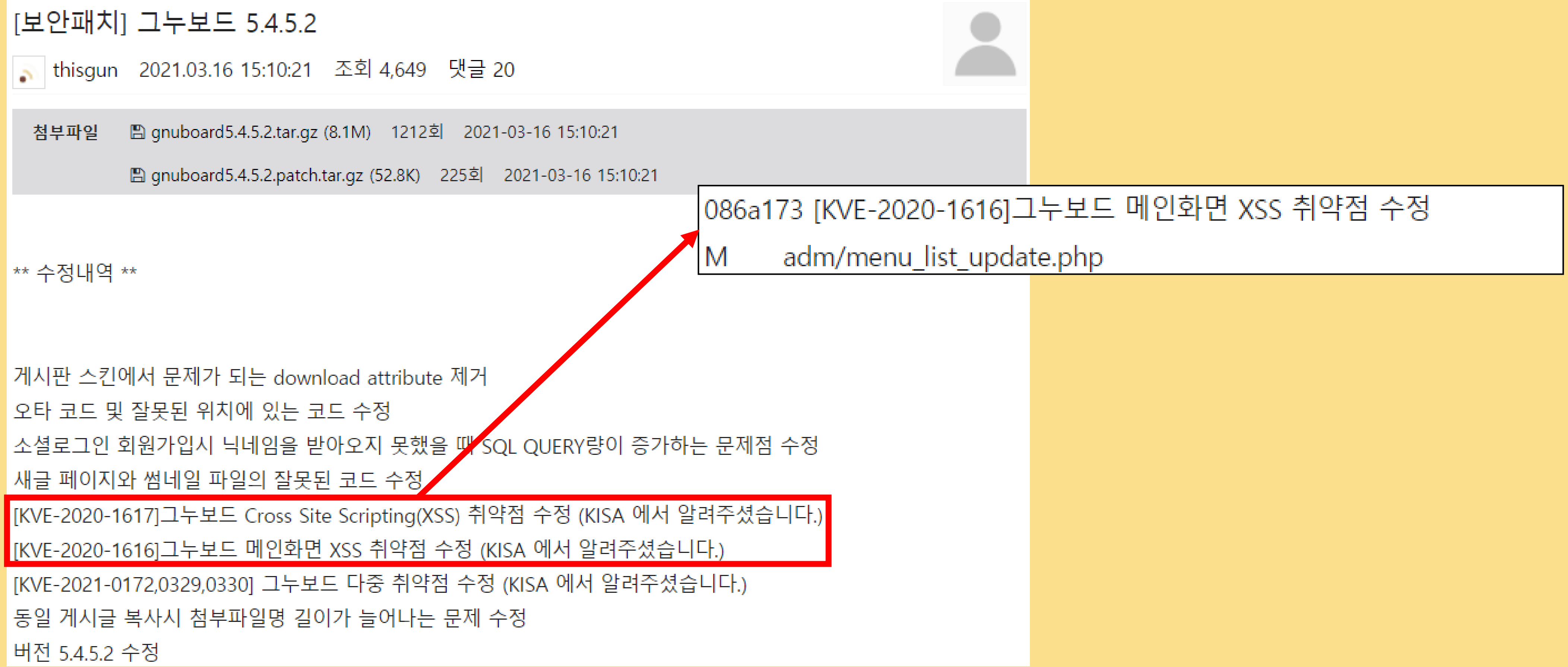
그누보드5 다운로드

전체 255 | RSS

SIR은 그누보드를 만들 뿐 프로그램의 설치, 운영방법, 설정문제에 관한 도움을 드리지는 않습니다.

번호	제목	작성일	조회
공지	동영상) 그누보드5 설치하기 ♥ 38	16.02.04	74797
공지	Github에서 그누보드5 최신버전 다운로드 ♥ 35	15.10.20	78082
253	그누보드 5.4.5.5 24	21.05.17	1316
252	그누보드 5.4.5.4 13	21.05.03	2481
251	그누보드 5.4.5.3 23	21.04.05	4144
250	[보안패치] 그누보드 5.4.5.2 20	21.03.16	4650
249	그누보드 5.4.5.1 29	21.02.05	8465
248	그누보드 5.4.4.9 21	21.01.26	4528

개요



[보안패치] 그누보드 5.4.5.2

thisgun 2021.03.16 15:10:21 조회 4,649 댓글 20

첨부파일 🖫 gnuboard5.4.5.2.tar.gz (8.1M) 1212회 2021-03-16 15:10:21

🖫 gnuboard5.4.5.2.patch.tar.gz (52.8K) 225회 2021-03-16 15:10:21

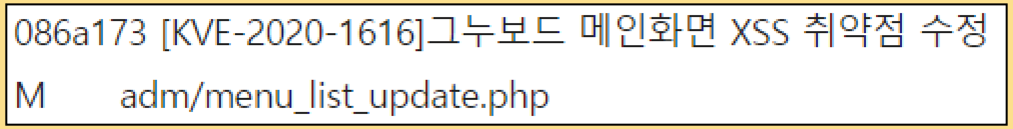
** 수정내역 **

게시판 스킨에서 문제가 되는 download attribute 제거
오타 코드 및 잘못된 위치에 있는 코드 수정
소셜로그인 회원가입시 닉네임을 받아오지 못했을 때 SQL QUERY량이 증가하는 문제점 수정
새글 페이지와 썸네일 파일의 잘못된 코드 수정
[KVE-2020-1617]그누보드 Cross Site Scripting(XSS) 취약점 수정 (KISA 에서 알려주셨습니다.)
[KVE-2020-1616]그누보드 메인화면 XSS 취약점 수정 (KISA 에서 알려주셨습니다.)
[KVE-2021-0172,0329,0330] 그누보드 다중 취약점 수정 (KISA 에서 알려주셨습니다.)
동일 게시글 복사시 첨부파일명 길이가 늘어나는 문제 수정
버전 5.4.5.2 수정

```
086a173 [KVE-2020-1616]그누보드 메인화면 XSS 취약점 수정
M       adm/menu_list_update.php
```

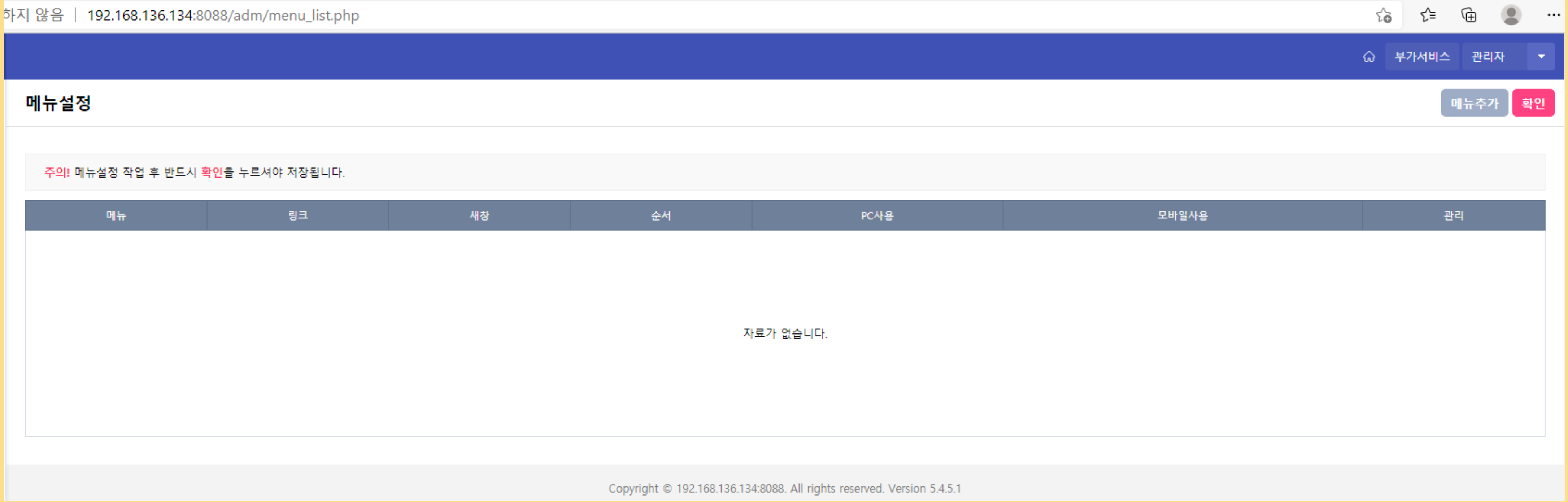
[KVE-2020-1616]

[KVE-2020-1616]



086a173 [KVE-2020-1616]그누보드 메인화면 XSS 취약점 수정

M   adm/menu_list_update.php



하지 않음 | 192.168.136.134:8088/adm/menu_list.php

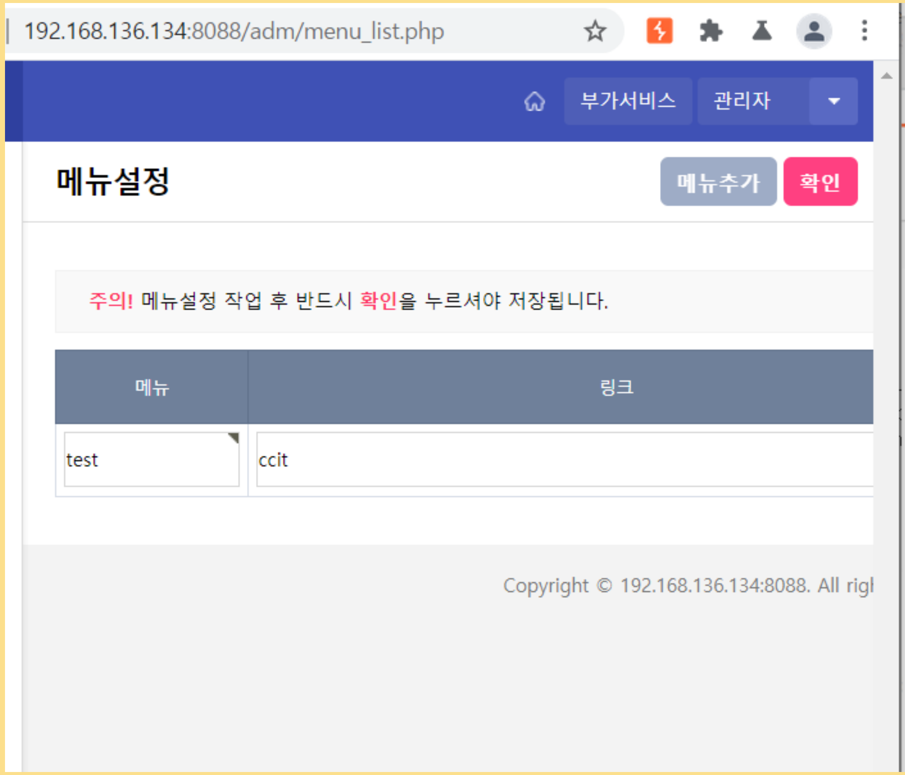
메뉴설정

주의! 메뉴설정 작업 후 반드시 확인을 누르셔야 저장됩니다.

메뉴	링크	새창	순서	PC사용	모바일사용	관리
자료가 없습니다.						

Copyright © 192.168.136.134:8088. All rights reserved. Version 5.4.5.1

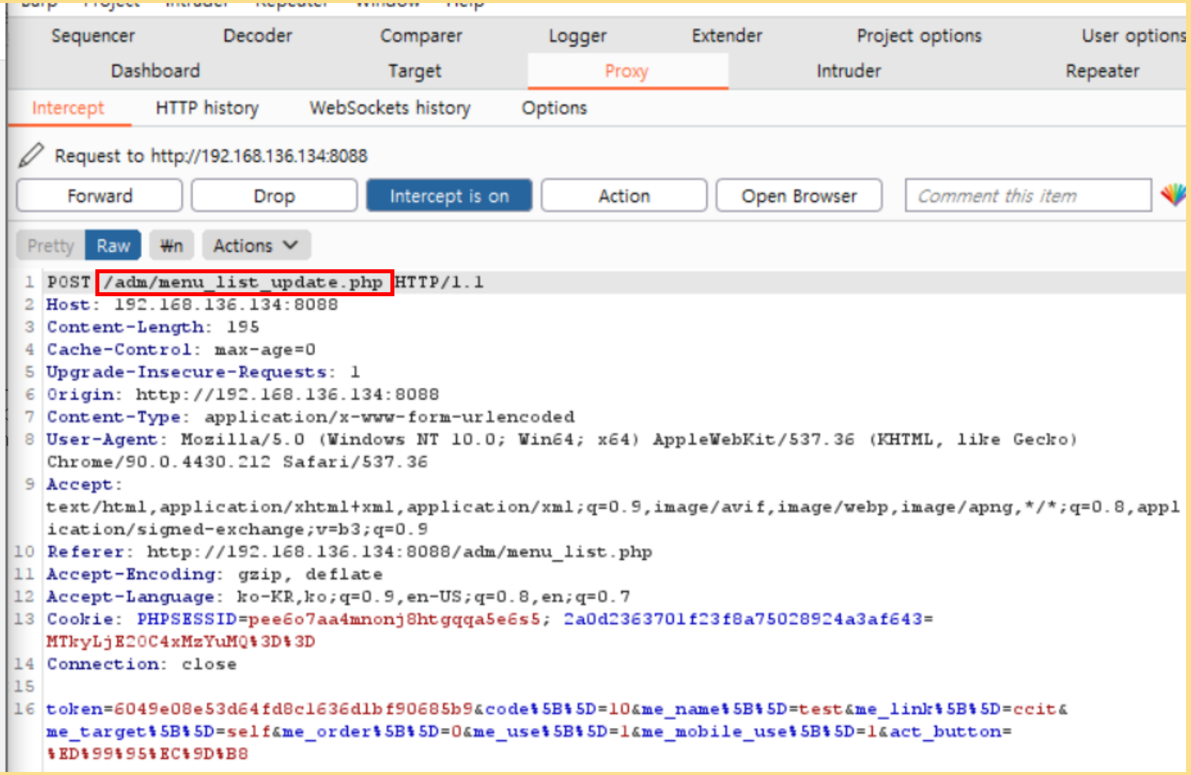
[KVE-2020-1616]



주의! 메뉴설정 작업 후 반드시 확인을 누르셔야 저장됩니다.

메뉴	링크
test	ccit

Copyright © 192.168.136.134:8088. All rigl

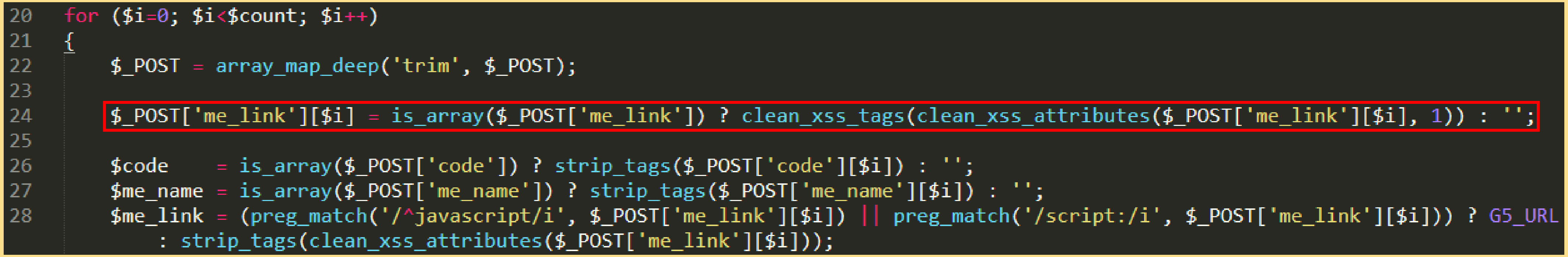


Request to http://192.168.136.134:8088

```
POST /adm/menu_list_update.php HTTP/1.1
Host: 192.168.136.134:8088
Content-Length: 195
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.136.134:8088
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
ication/signed-exchange;v=b3;q=0.9
Referer: http://192.168.136.134:8088/adm/menu_list.php
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PHPSESSID=pee6o7aa4mnonj8htgqqa5e6s5; 2a0d2363701f23f8a75028924a3af643=
MTkyLjE2OC4xMzYuMQ%3D%3D
Connection: close

token=6049e08e53d64fd8c1636d1bf90685b9&code%5B%5D=10&me_name%5B%5D=test&me_link%5B%5D=ccit&
me_target%5B%5D=self&me_order%5B%5D=0&me_use%5B%5D=1&me_mobile_use%5B%5D=1&act_button=
%ED%99%95%EC%9D%B8
```

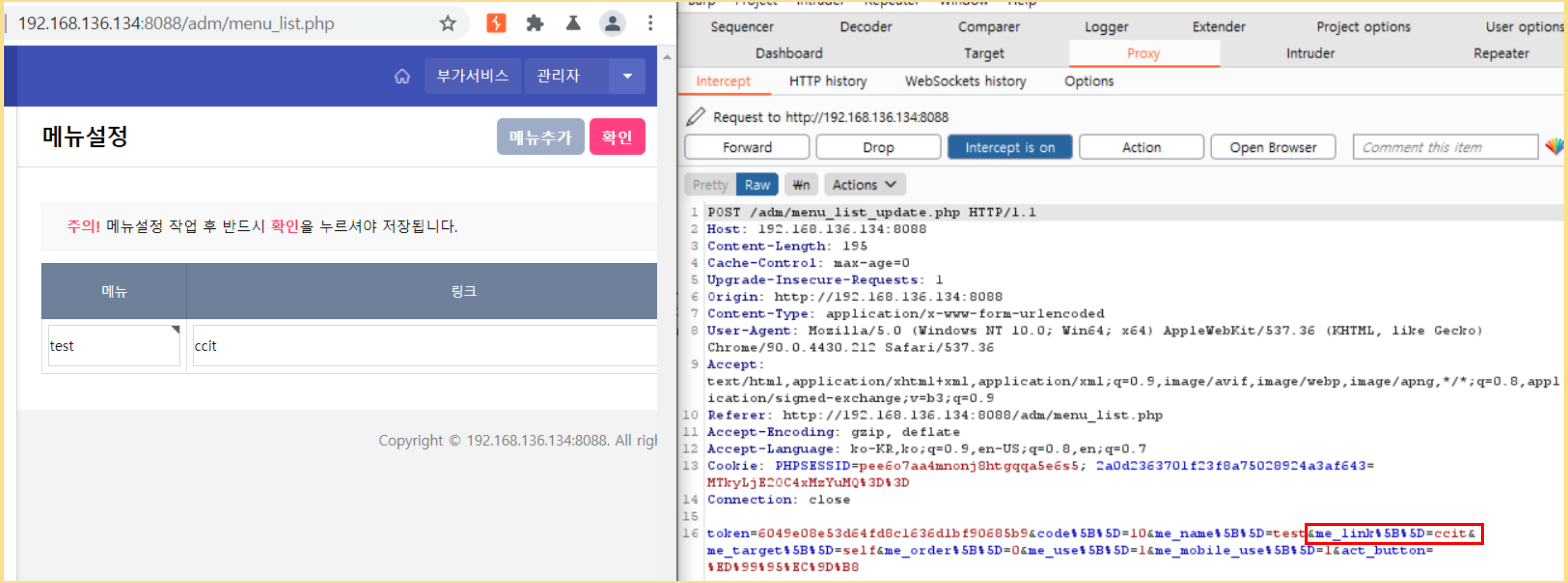
[KVE-2020-1616]

menu_list_update.php



```
for ($i=0; $i<$count; $i++)
{
    $_POST = array_map_deep('trim', $_POST);

    $_POST['me_link'][$i] = is_array($_POST['me_link']) ? clean_xss_tags(clean_xss_attributes($_POST['me_link'][$i], 1)) : '';

    $code    = is_array($_POST['code']) ? strip_tags($_POST['code'][$i]) : '';
    $me_name = is_array($_POST['me_name']) ? strip_tags($_POST['me_name'][$i]) : '';
    $me_link = (preg_match('/^javascript/i', $_POST['me_link'][$i]) || preg_match('/script:/i', $_POST['me_link'][$i])) ? G5_URL
        : strip_tags(clean_xss_attributes($_POST['me_link'][$i]));
```

[KVE-2020-1616]



메뉴설정

주의! 메뉴설정 작업 후 반드시 확인을 누르셔야 저장됩니다.

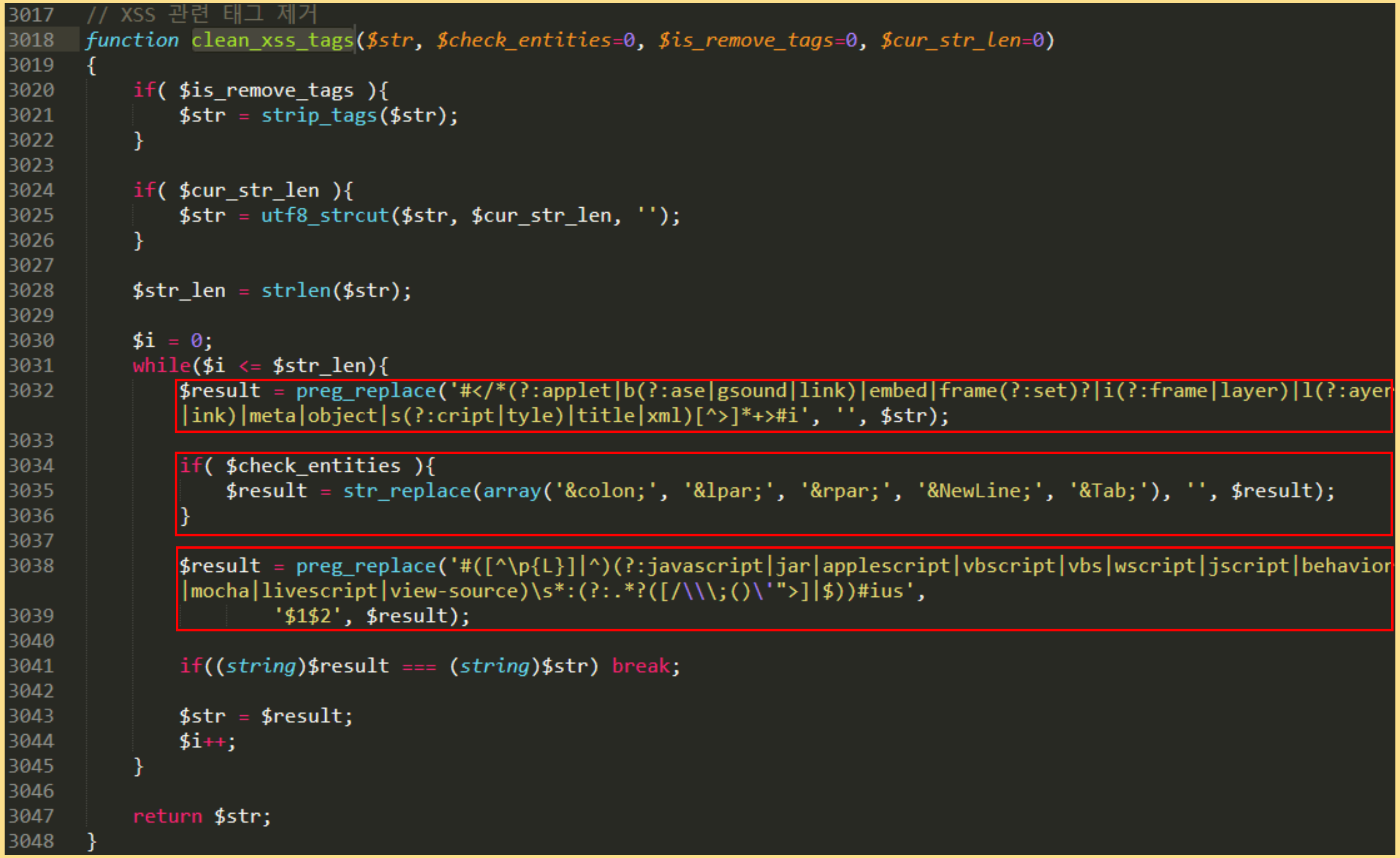
메뉴	링크
test	ccit

Copyright © 192.168.136.134:8088. All rigl

```
POST /adm/menu_list_update.php HTTP/1.1
Host: 192.168.136.134:8088
Content-Length: 195
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.136.134:8088
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
ication/signed-exchange;v=b3;q=0.9
Referer: http://192.168.136.134:8088/adm/menu_list.php
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PHPSESSID=pee6o7aa4mnonj8htgqqa5e6s5; 2a0d2363701f23f8a75028924a3af643=
MTkyLjE2OC4xMzYuMQ%3D%3D
Connection: close

token=6049e08e53d64fd8c1636d1bf90685b9&code%5B%5D=10&me_name%5B%5D=test&me_link%5B%5D=ccit&
me_target%5B%5D=self&me_order%5B%5D=0&me_use%5B%5D=1&me_mobile_use%5B%5D=1&act_button=
%ED%99%95%EC%9D%B8
```

[KVE-2020-1616]

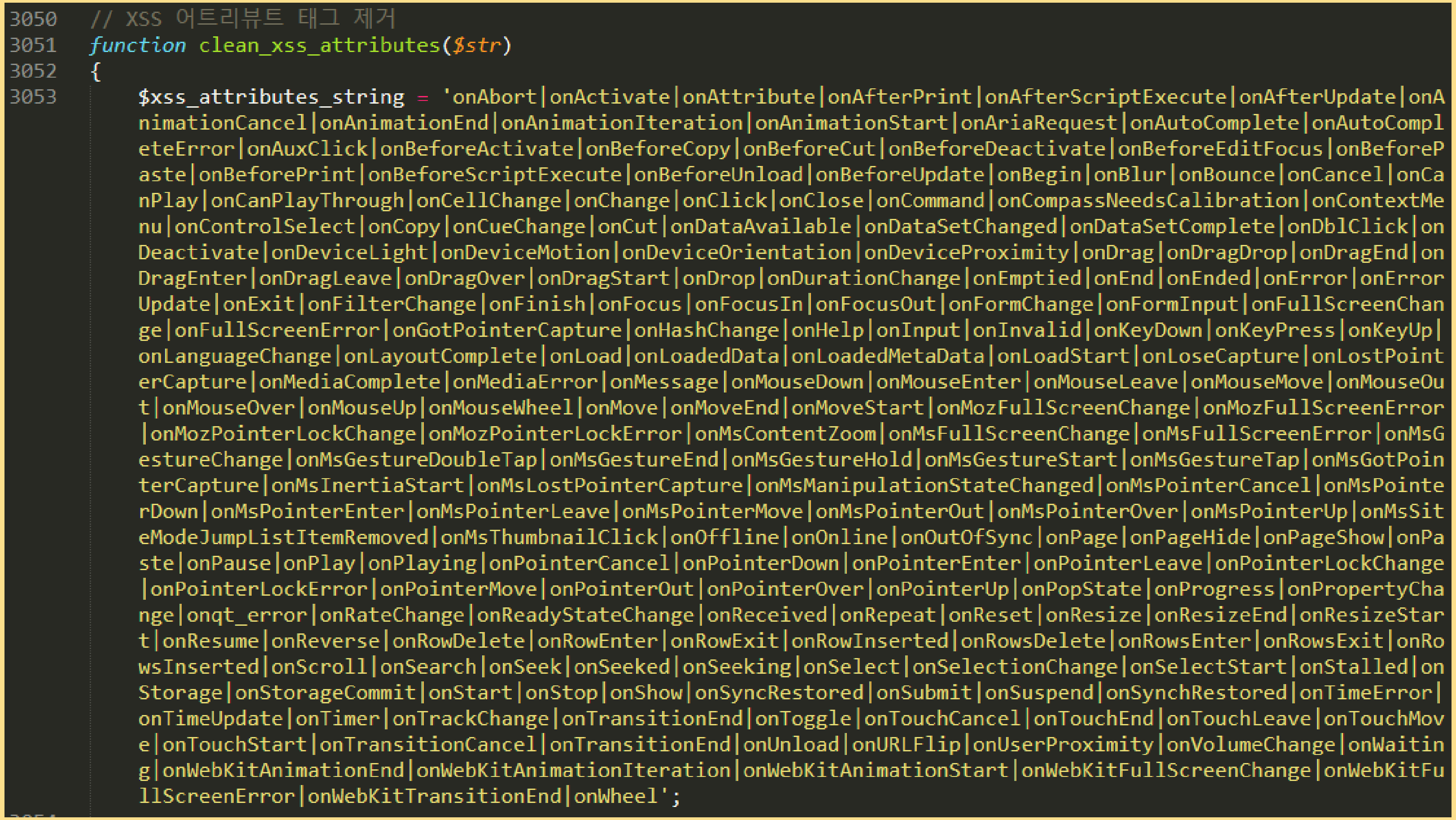
common.lib.php



```php
// XSS 관련 태그 제거
function clean_xss_tags($str, $check_entities=0, $is_remove_tags=0, $cur_str_len=0)
{
    if( $is_remove_tags ){
        $str = strip_tags($str);
    }

    if( $cur_str_len ){
        $str = utf8_strcut($str, $cur_str_len, '');
    }

    $str_len = strlen($str);

    $i = 0;
    while($i <= $str_len){
        $result = preg_replace('#</*(?:applet|b(?:ase|gsound|link)|embed|frame(?:set)?|i(?:frame|layer)|l(?:ayer
        |ink)|meta|object|s(?:cript|tyle)|title|xml)[^>]*+>#i', '', $str);

        if( $check_entities ){
            $result = str_replace(array('&colon;', '&lpar;', '&rpar;', '&NewLine;', '&Tab;'), '', $result);
        }

        $result = preg_replace('#([^\p{L}]|^)(?:javascript|jar|applescript|vbscript|vbs|wscript|jscript|behavior
        |mocha|livescript|view-source)\s*:(?:.*?([/\\\;()\'">]|$))#ius',
                '$1$2', $result);

        if((string)$result === (string)$str) break;

        $str = $result;
        $i++;
    }

    return $str;
}
```

[KVE-2020-1616]

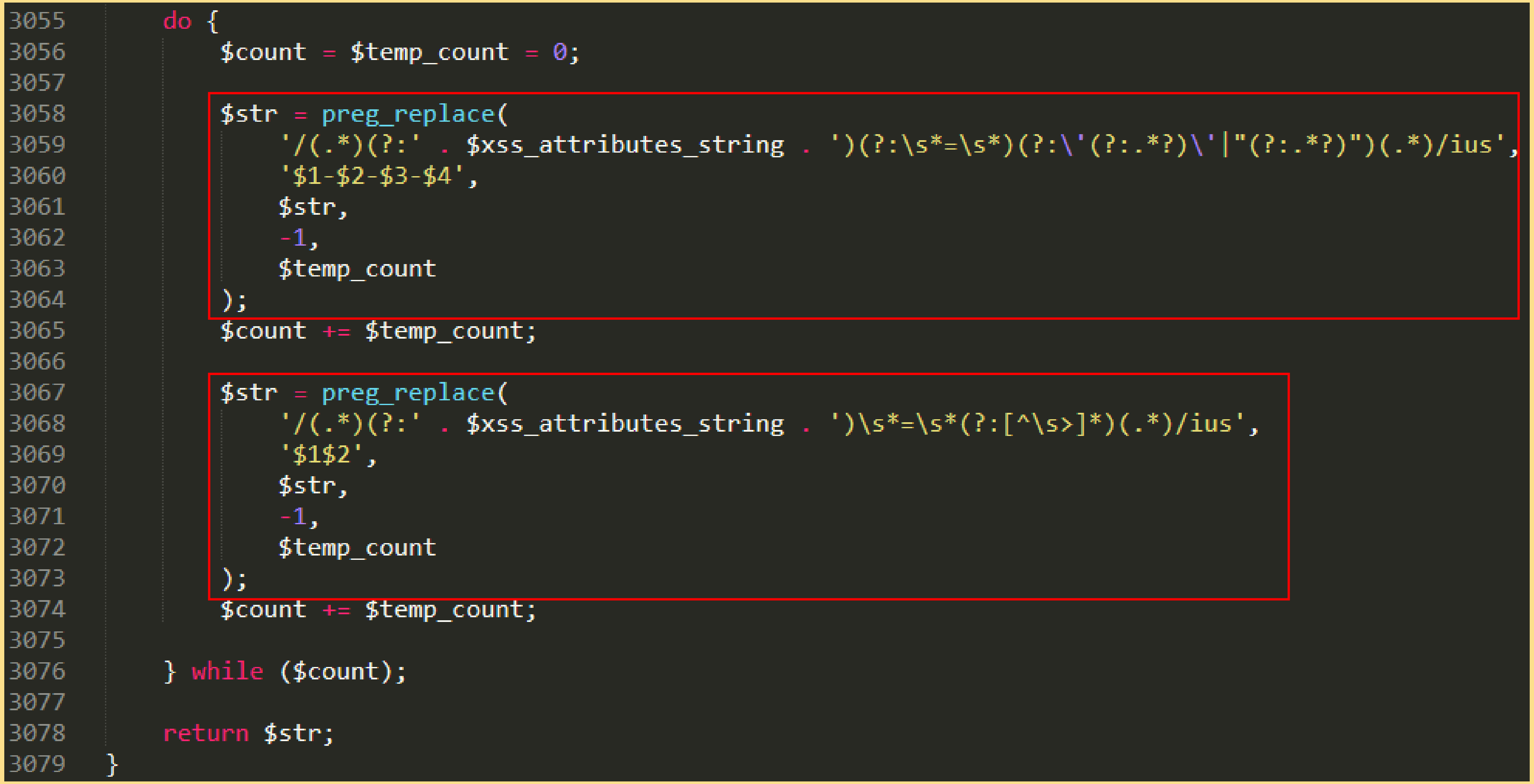
common.lib.php



```php
// XSS 어트리뷰트 태그 제거
function clean_xss_attributes($str)
{
    $xss_attributes_string = 'onAbort|onActivate|onAttribute|onAfterPrint|onAfterScriptExecute|onAfterUpdate|onAnimationCancel|onAnimationEnd|onAnimationIteration|onAnimationStart|onAriaRequest|onAutoComplete|onAutoCompleteError|onAuxClick|onBeforeActivate|onBeforeCopy|onBeforeCut|onBeforeDeactivate|onBeforeEditFocus|onBeforePaste|onBeforePrint|onBeforeScriptExecute|onBeforeUnload|onBeforeUpdate|onBegin|onBlur|onBounce|onCancel|onCanPlay|onCanPlayThrough|onCellChange|onChange|onClick|onClose|onCommand|onCompassNeedsCalibration|onContextMenu|onControlSelect|onCopy|onCueChange|onCut|onDataAvailable|onDataSetChanged|onDataSetComplete|onDblClick|onDeactivate|onDeviceLight|onDeviceMotion|onDeviceOrientation|onDeviceProximity|onDrag|onDragDrop|onDragEnd|onDragEnter|onDragLeave|onDragOver|onDragStart|onDrop|onDurationChange|onEmptied|onEnd|onEnded|onError|onErrorUpdate|onExit|onFilterChange|onFinish|onFocus|onFocusIn|onFocusOut|onFormChange|onFormInput|onFullScreenChange|onFullScreenError|onGotPointerCapture|onHashChange|onHelp|onInput|onInvalid|onKeyDown|onKeyPress|onKeyUp|onLanguageChange|onLayoutComplete|onLoad|onLoadedData|onLoadedMetaData|onLoadStart|onLoseCapture|onLostPointerCapture|onMediaComplete|onMediaError|onMessage|onMouseDown|onMouseEnter|onMouseLeave|onMouseMove|onMouseOut|onMouseOver|onMouseUp|onMouseWheel|onMove|onMoveEnd|onMoveStart|onMozFullScreenChange|onMozFullScreenError|onMozPointerLockChange|onMozPointerLockError|onMsContentZoom|onMsFullScreenChange|onMsFullScreenError|onMsGestureChange|onMsGestureDoubleTap|onMsGestureEnd|onMsGestureHold|onMsGestureStart|onMsGestureTap|onMsGotPointerCapture|onMsInertiaStart|onMsLostPointerCapture|onMsManipulationStateChanged|onMsPointerCancel|onMsPointerDown|onMsPointerEnter|onMsPointerLeave|onMsPointerMove|onMsPointerOut|onMsPointerOver|onMsPointerUp|onMsSiteModeJumpListItemRemoved|onMsThumbnailClick|onOffline|onOnline|onOutOfSync|onPage|onPageHide|onPageShow|onPaste|onPause|onPlay|onPlaying|onPointerCancel|onPointerDown|onPointerEnter|onPointerLeave|onPointerLockChange|onPointerLockError|onPointerMove|onPointerOut|onPointerOver|onPointerUp|onPopState|onProgress|onPropertyChange|onqt_error|onRateChange|onReadyStateChange|onReceived|onRepeat|onReset|onResize|onResizeEnd|onResizeStart|onResume|onReverse|onRowDelete|onRowEnter|onRowExit|onRowInserted|onRowsDelete|onRowsEnter|onRowsExit|onRowsInserted|onScroll|onSearch|onSeek|onSeeked|onSeeking|onSelect|onSelectionChange|onSelectStart|onStalled|onStorage|onStorageCommit|onStart|onStop|onShow|onSyncRestored|onSubmit|onSuspend|onSynchRestored|onTimeError|onTimeUpdate|onTimer|onTrackChange|onTransitionEnd|onToggle|onTouchCancel|onTouchEnd|onTouchLeave|onTouchMove|onTouchStart|onTransitionCancel|onTransitionEnd|onUnload|onURLFlip|onUserProximity|onVolumeChange|onWaiting|onWebKitAnimationEnd|onWebKitAnimationIteration|onWebKitAnimationStart|onWebKitFullScreenChange|onWebKitFullScreenError|onWebKitTransitionEnd|onWheel';
```

[KVE-2020-1616]

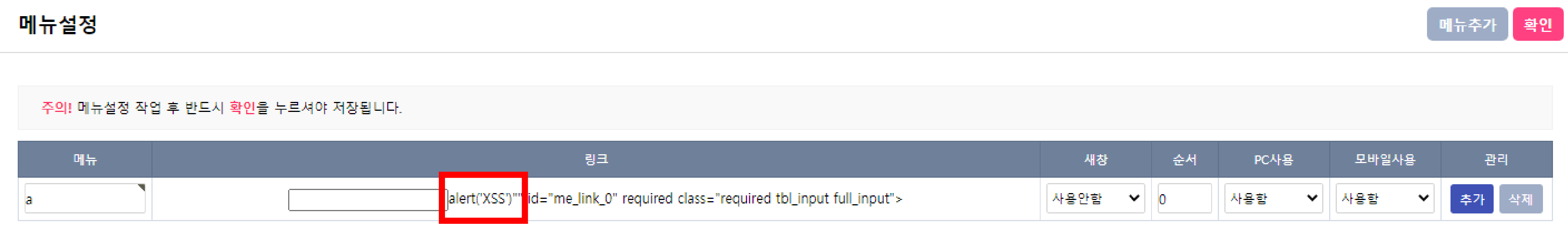
common.lib.php



```
    do {
        $count = $temp_count = 0;

        $str = preg_replace(
            '/(.*)(?:' . $xss_attributes_string . ')(?:\s*=\s*)(?:\'(?:.*?)\'|"(?:.*?)")(.*)/ius',
            '$1-$2-$3-$4',
            $str,
            -1,
            $temp_count
        );
        $count += $temp_count;

        $str = preg_replace(
            '/(.*)(?:' . $xss_attributes_string . ')\s*=\s*(?:[^\s>]*)(.*)/ius',
            '$1$2',
            $str,
            -1,
            $temp_count
        );
        $count += $temp_count;

    } while ($count);

    return $str;
}
```

[KVE-2020-1616]

"><script>alert('XSS')</script>"

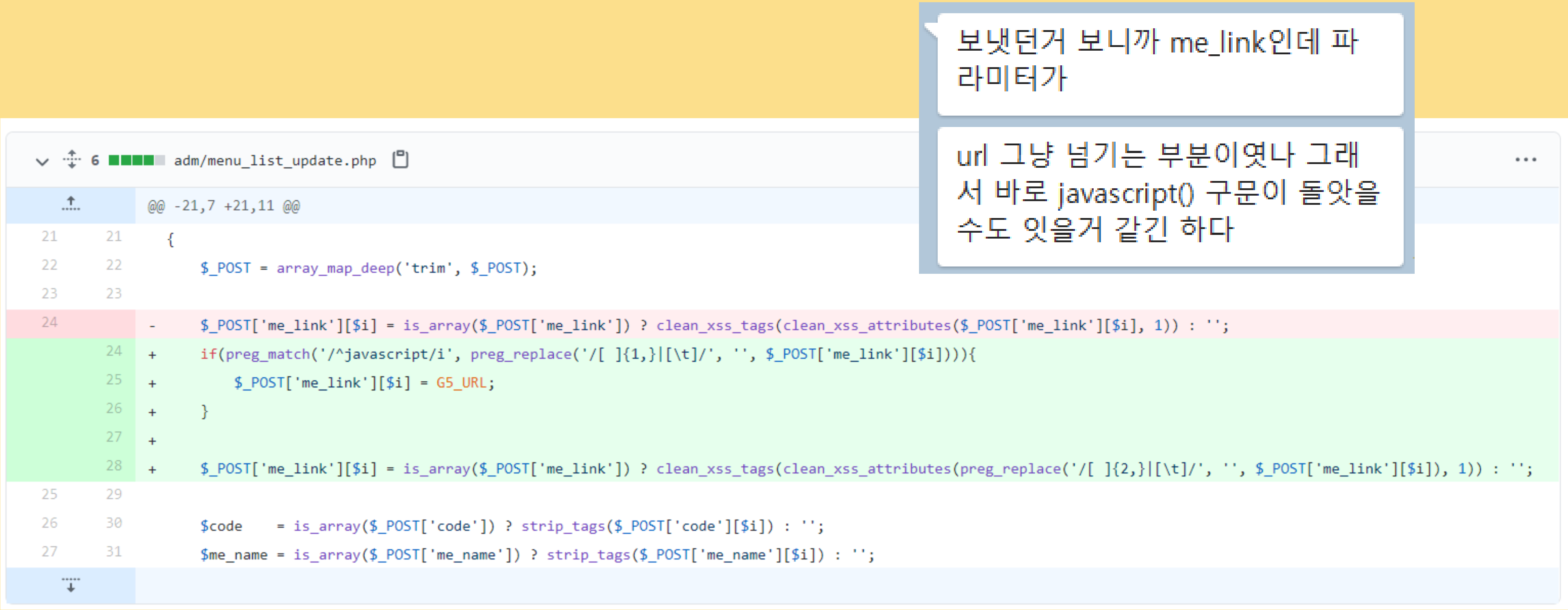


메뉴설정

주의! 메뉴설정 작업 후 반드시 확인을 누르셔야 저장됩니다.

메뉴	링크	새창	순서	PC사용	모바일사용	관리
a	alert('XSS')"" id="me_link_0" required class="required tbl_input full_input">	사용안함	0	사용함	사용함	추가 삭제

[KVE-2020-1616]



보냇던거 보니까 me_link인데 파라미터가

url 그냥 넘기는 부분이엿나 그래서 바로 javascript() 구문이 돌앗을수도 잇을거 같긴 하다

```
@@ -21,7 +21,11 @@
     {
         $_POST = array_map_deep('trim', $_POST);

-        $_POST['me_link'][$i] = is_array($_POST['me_link']) ? clean_xss_tags(clean_xss_attributes($_POST['me_link'][$i], 1)) : '';
+        if(preg_match('/^javascript/i', preg_replace('/[ ]{1,}|[\t]/', '', $_POST['me_link'][$i]))){
+            $_POST['me_link'][$i] = G5_URL;
+        }
+
+        $_POST['me_link'][$i] = is_array($_POST['me_link']) ? clean_xss_tags(clean_xss_attributes(preg_replace('/[ ]{2,}|[\t]/', '', $_POST['me_link'][$i]), 1)) : '';

         $code    = is_array($_POST['code']) ? strip_tags($_POST['code'][$i]) : '';
         $me_name = is_array($_POST['me_name']) ? strip_tags($_POST['me_name'][$i]) : '';
```

Thank you