XCTF两个PHP代码审计的笔记

转载

weixin_30892889 于 2019-09-30 13:30:00 发布 103 收藏
文章标签： php 数据库
原文链接：http://www.cnblogs.com/BOHB-yunying/p/10685339.html

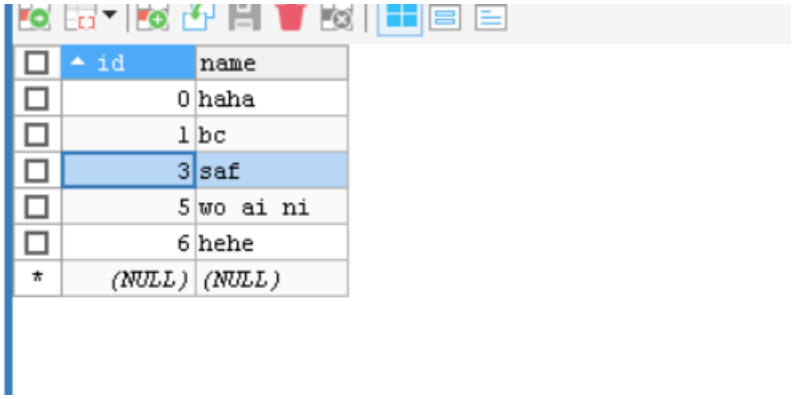
题目源码如下，考点是输入的$id和$row['id']的区别

```php
if(isset($_POST['id']) && isset($_POST['ps'])){
  include("flag.php");

  mysql_connect("localhost","adog","adog123");
  mysql_select_db ("adog");
  mysql_query("set names utf8");

  $key = flag();

  $id = mysql_real_escape_string(trim($_POST['id']));
  $ps = mysql_real_escape_string(trim($_POST['ps']));

  $row=mysql_fetch_array(mysql_query("select * from users where id='$id' and ps=md5('$ps')"));

  if(isset($row['id'])){
   if($id=='adog'){
    echo "your account is blocked";
   }else{
    echo "login ok"."<br ";
    echo "Password : ".$key;
   }
  }else{
   echo "wrong..";
  }
 }
?>
```

关键在于红框内，可以知道题目的payload是要让$row['id']存在，查询的到数据，并且要让POST的id不能与adog相同。那显而易见，肯定是要你输入的id！==adog，并且需要绕过$row['id']的限制。

从P牛blog里，学到的一手姿势。自己用mysql FUZZ测试下，从这里可以查看$row['id']和$id的区别

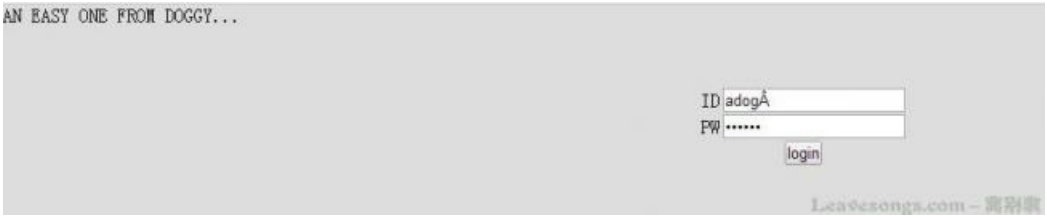
```php
<?php
mysql_connect("localhost","root","root");
mysql_select_db ("test");
mysql_query("set names utf8");
for($i = 0 ; $i < 256 ; $i++){
    $c = chr($i);
    $name = mysql_real_escape_string('hehe' . $c);
    $sql = "SELECT * FROM `people` WHERE `name` = '{$name}'";
    $result=mysql_query($sql);$row = mysql_fetch_array($result);
    if ($row['name'] == 'hehe') {
        echo "{$c} <br/>";
    }
}
# P牛 bloghttps://www.leavesongs.com/PENETRATION/Mini-XCTF-Writeup.html
?>
#如果在name后面加上一个字符，在mysql里查询，如果查到的和不加这个字符查出来的行相同，则输出。
```



id	name
0	haha
1	bc
3	saf
5	wo ai ni
6	hehe
(NULL)	*(NULL)*

我在数据表中插入了这些数据

Warning: mysql_fetch_array() expects parameter 1 to be re
Â
Ã
Ä
Å
Æ
Ç
È
É
Ê
Ë
Ì
Í
Î
Ï
Ð
Ñ
Ò
Ó
Ô
Õ
Ö
×
Ø
Ù
Ú
Û
Ü
Ý
Þ
ß
à
á



也就是说输入的id是adogÂ ,但是在mysql_fetch_array(mysql_query($sql))，查询并且关联数组后，数组内键值为id的数组值仍为adog,所以$row['id']存在,因此绕过了$id==adog，并且还使$row['id']值存在.

那个fuzz已经充分的证明了。

转载于:https://www.cnblogs.com/BOHB-yunying/p/10685339.html