

实验吧-程序逻辑问题writeup

原创

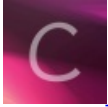
tm阿信 于 2017-08-27 09:10:01 发布 9178 收藏 1

分类专栏: [Web安全](#) 文章标签: [ctf西普实验吧](#)

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/he_and/article/details/77618429

版权



[Web安全](#) 专栏收录该内容

74 篇文章 14 订阅

订阅专栏

1. 程序逻辑问题

题目提示是程序逻辑问题, 那一定涉及到源码审计嘛, F12查看网页源代码:

这儿不就藏着源码吗, 构造URL访问index.txt的如下源码:

```
<html>
```

```
<head>
```

```
welcome to simplexue
```

```
</head>
```

```
<body>
```

```
<?php
```

```
if($_POST[user] && $_POST[pass]) {
```

```
    $conn= mysql_connect("*****", "*****", "*****");
```

```
    mysql_select_db("phpformysql")or die("Could not select database");
```

```
    if($conn->connect_error) {
```

```
        die("Connectionfailed: " . mysql_error($conn));
```

```
    }
```

```
    $user = $_POST[user];
```

```
    $pass = md5($_POST[pass]);
```

```

$sql = "select pw from php where user='$user'";

$query = mysql_query($sql);

if (!$query) {
    printf("Error: %s\n", mysql_error($conn));
    exit();
}

$row = mysql_fetch_array($query, MYSQL_ASSOC);
//echo $row["pw"];

if (($row[pw] && (!strcasecmp($pass, $row[pw]))) {
    echo "<p>Logged in! Key:***** </p>";
}

else {
    echo("<p>Log in failure!</p>");

}

}

?>

<form method=post action=index.php>
<input type=text name=user value="Username">
<input type=password name=pass value="Password">
<input type=submit>
</form>
</body>
<a href="index.txt">
</html>

```

根据源码可以看到两处特别需要重视的地方，我已标红，很明显该sql语句存在注入漏洞，但是密码栏不能通过一般的注入来绕过，但是可以发现，只要满足了 (**\$row[pw]**) && (!strcasecmp(\$pass,\$row[pw])**就可以拿到flag**，也就是说，我们输入的\$pass与从数据库取出来的pw一致就行，我们可以控制\$pass的值，但是貌似不知道数据库中pw的值，但是我们可以直接用union select '某一个经过md5加密后的字符串'#来自己随意设定密码，注意这里一定是经过md5加密，不然会出错。

构造语句:' and 0=1 union select '529CA8050A00180790CF88B63468826A'#

密码: hehe

就拿到flag了。

2.



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)