# 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



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

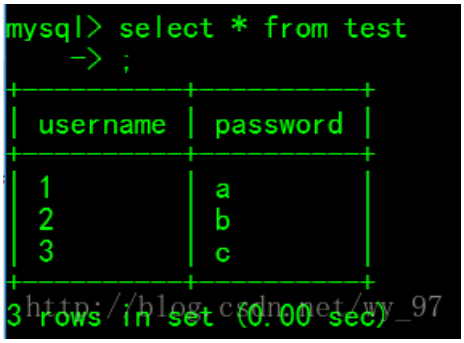
```
$sql = “select user from flag where user=’‘=’’ and password=’‘=’‘”;
```

大佬们对此的解释为：

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

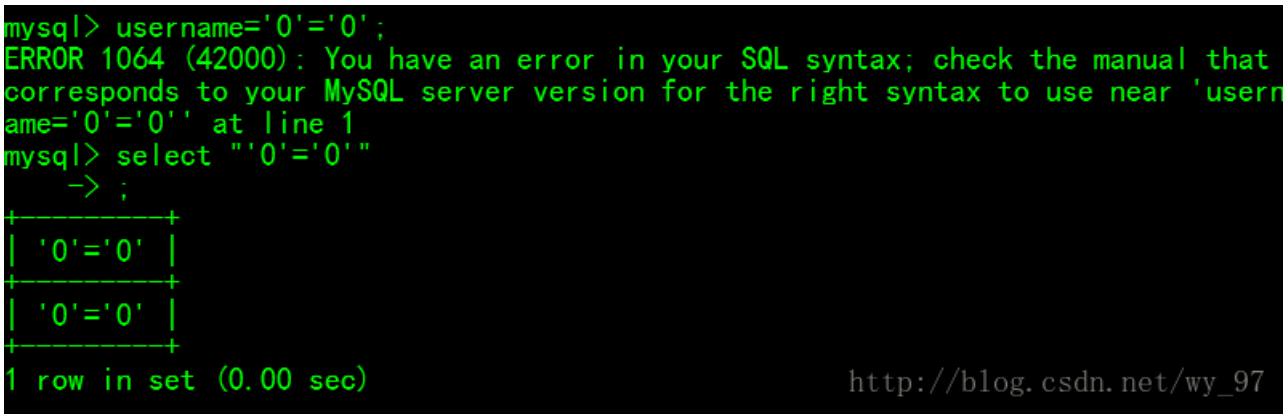
对于这个地方还是有点难以理解，自己在本地mysql数据库创建了一个test，进行了一些测试：

这是test表内的内容:



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：


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：




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

很详细