堆叠注入

1、堆叠注入定义

Stacked injections(堆叠注入)从名词的含义就可以看到应该是一堆 sql 语句(多条)一起执行。而在真实的运用中也是这样的,我们知道在 mysql 中, 主要是命令行中,每一条语句结尾加；表示语句结束。这样我们就想到了是不是可以多句一起使用。这个叫做 stacked injection。

2、堆叠注入原理

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 语句后继续构造下一条语句,会不会一起执行？因此这个想法也就造就了堆叠注入。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。例如以下这个例子。用户输入：1；DELETE FROM products

服务器端生成的 sql 语句为：

select * from users where productid=1;DELETE FROM users

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。

堆叠注入的局限性在于并不是每一个环境下都可以执行,虽然我们前面提到了堆叠查询可以执行任意的 sql 语句，但是这种注入方式并不是十分的完美的。在我们的 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。

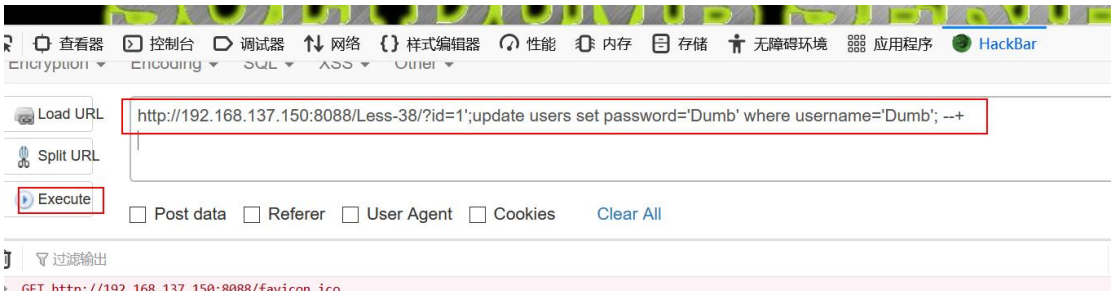
3、堆叠注入演示

Less-38

首先看 id 为 1 的用户信息

然后发送堆叠注入

http://192.168.137.150:8088/Less-38/?id=1';update users set password='Dumb' where username='Dumb'; --+



再次查询，密码改变

4、流量分析

Sql 语句的堆叠流量

破坏语句堆叠