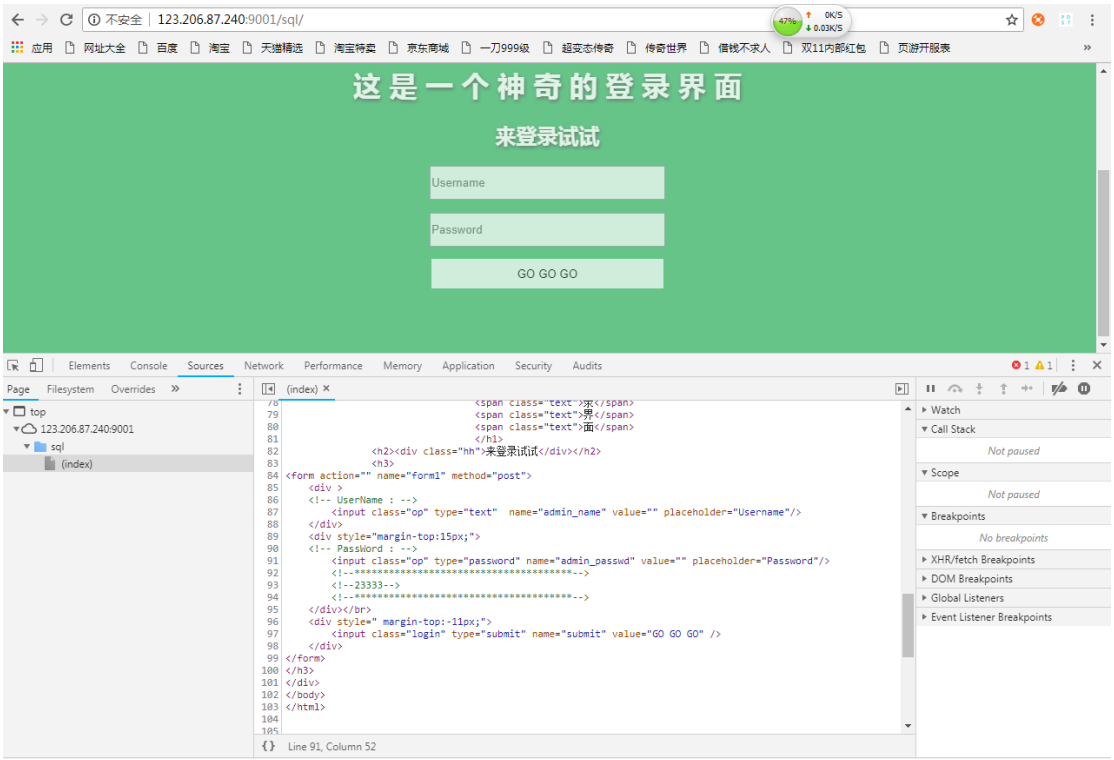
参考

https://blog.csdn.net/qq_38412357/article/details/79559039

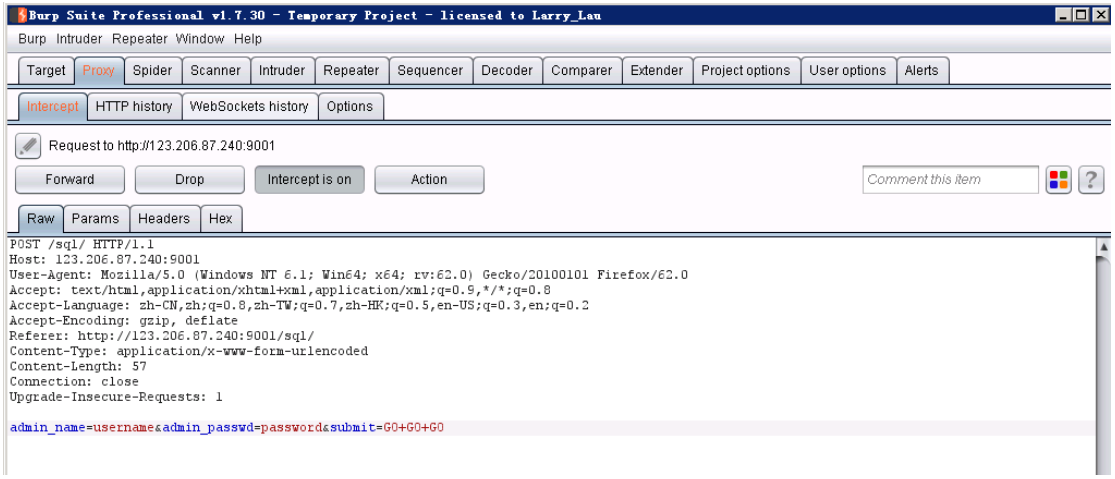
http://123.206.87.240:9001/sql/

查看源码



是 post 提交，url 明显提示是个 sql 注入，由于 post 提交，要 sql 和 burp 结合起来使用。

首先 burp 抓包，抓到包后选择存到 txt 文件中：（随便输入账号密码）



保存到了 c 盘的 test1.txt 里

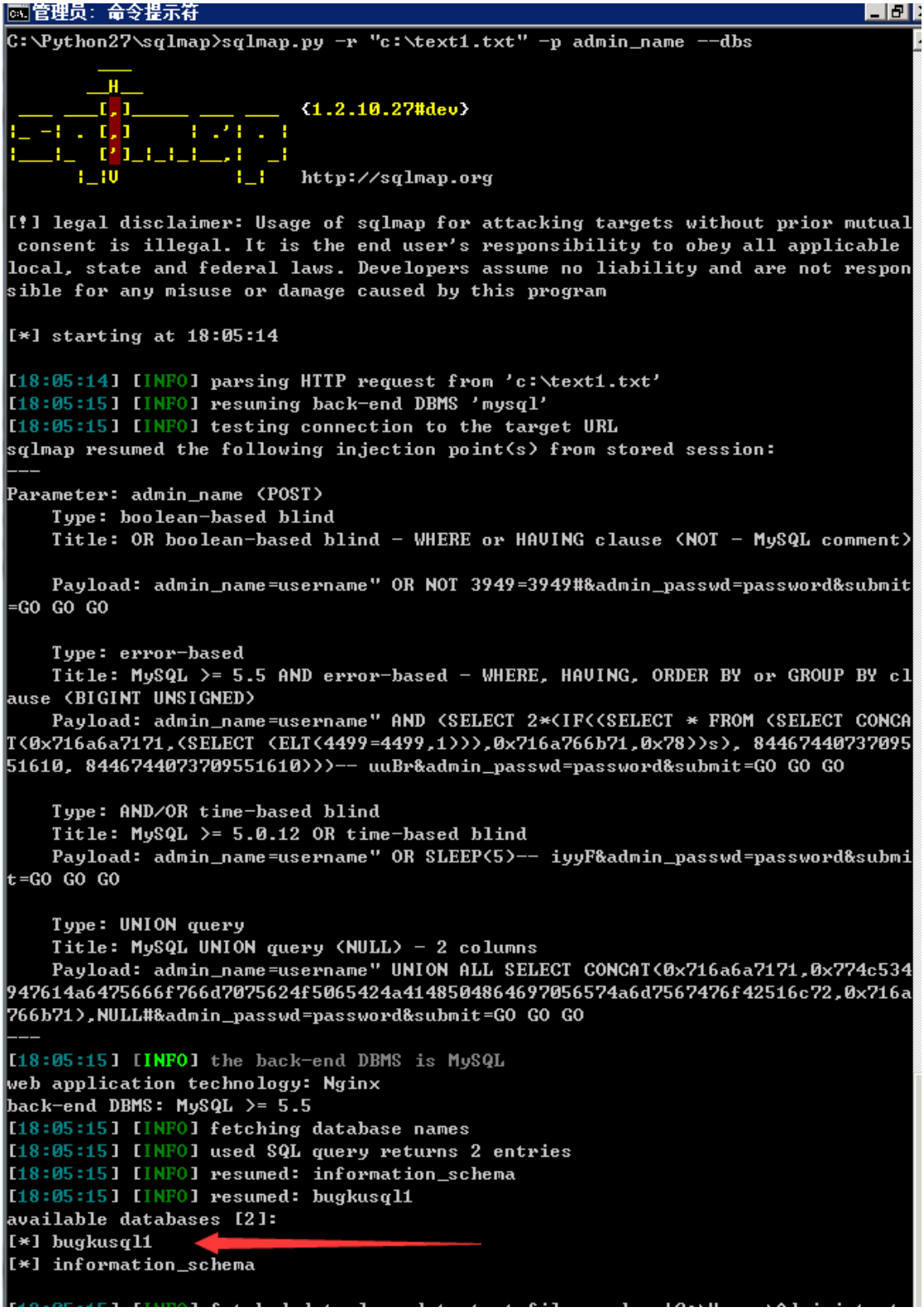
注：Windows 下 sqlmap 安装方法

https://blog.csdn.net/lijia111111/article/details/54755009

然后打开 sqlmap，输入指令：sqlmap.py -r "c:\text1.txt" -p admin_name –dbs

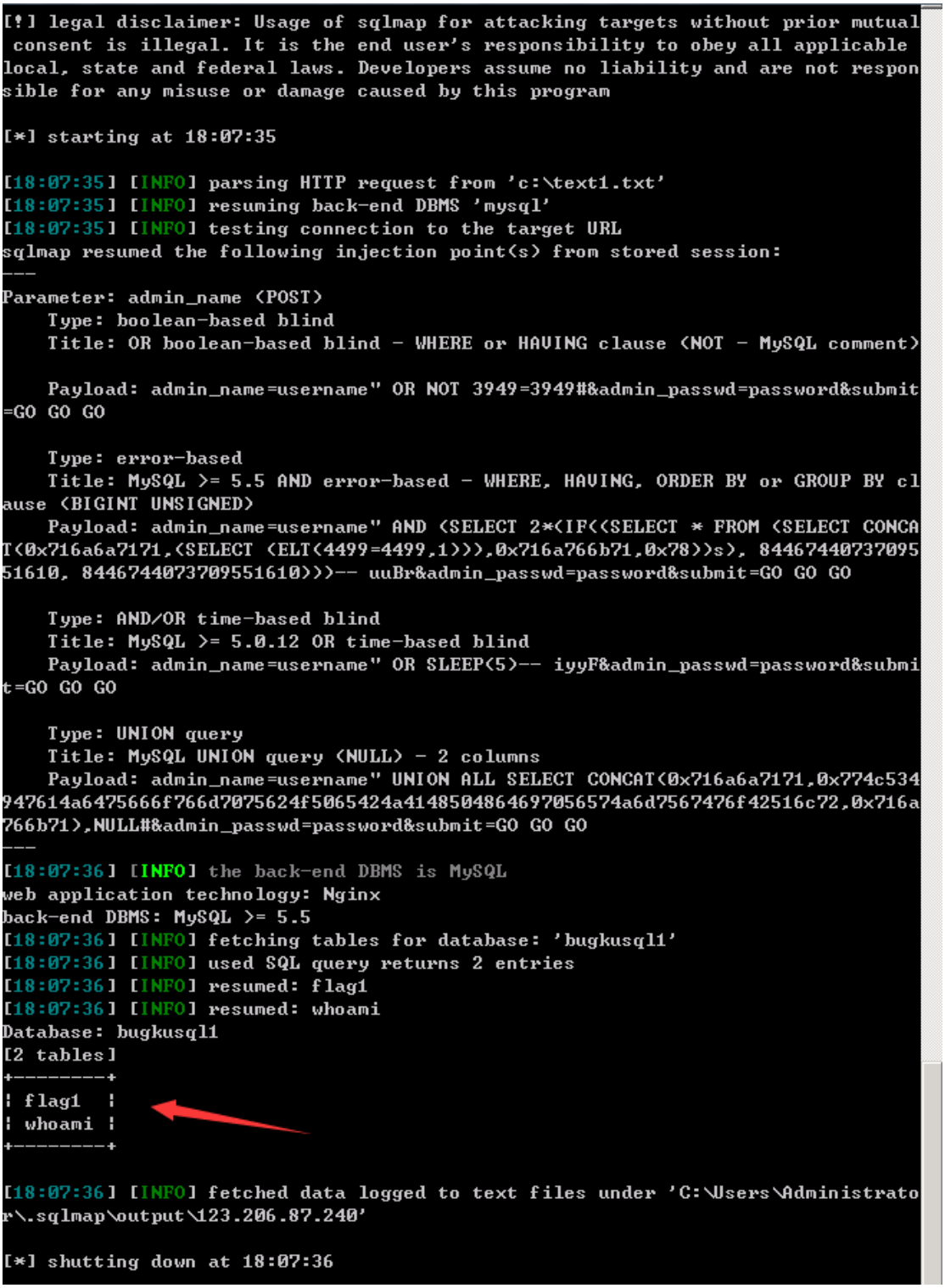
解释一下 -r 是读文件 后面是刚才保存的绝对路径，-p 是参数，也就是注入点（选了 admin_name 是注入点） --dbs 意思是想获取数据库名字

可以看到 sqlmap 获得了数据库的名字：



应该是这个 bugkul1，再继续爆表，命令：

sqlmap.py -r "c:\text1.txt" -D bugkusql1 -p admin_name –tables



解释：-D 是表示选择了后面的这个数据库 --tables 是想获取表

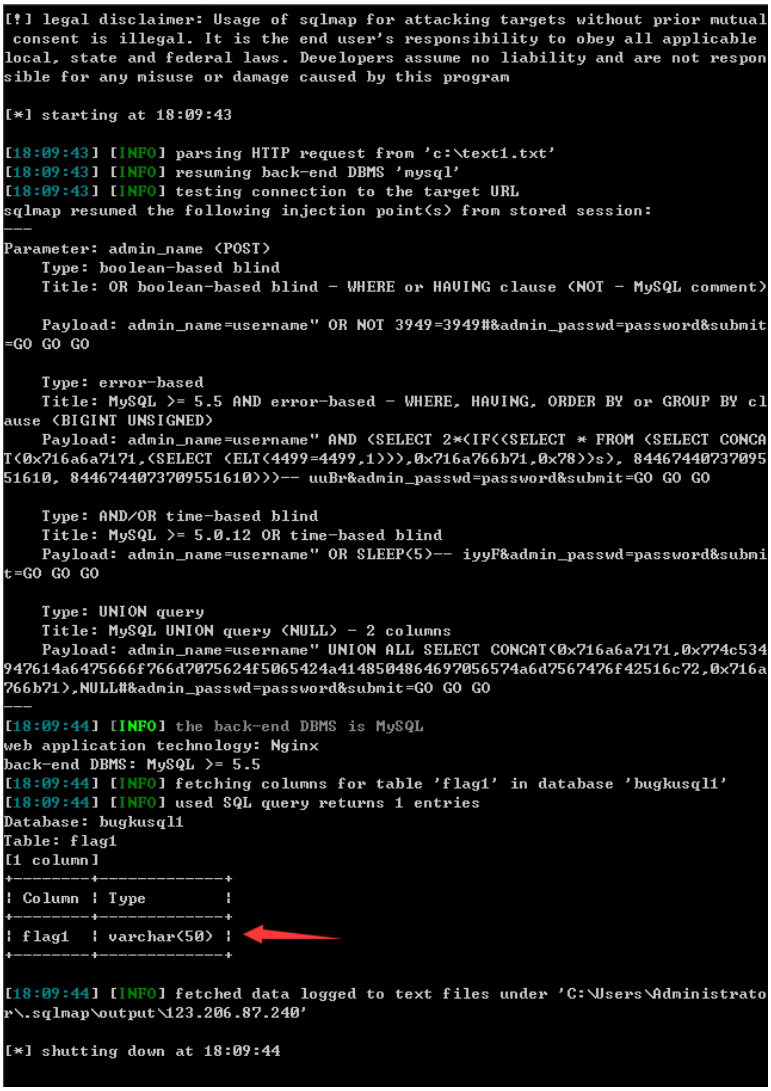
可以看到爆出了表：

应该在 flag1 这个表里，继续爆列名：

命令：sqlmap.py -r "c:\text1.txt" -D bugkusql1 -T flag1 -p admin_name --columns

解释类似上面 不过加了一个-T 指定表

可以发现爆出了列名：



flag1 这个列 最后查字段 命令：

sqlmap.py -r "c:\text1.txt" -D bugkusql1 -T flag1 -C flag1 -p admin_name –dump

解释：同上面 --dump 是获取字段的命令

（在这过程中可能会让你选择 Y 或者 N 我直接回车的）

可以看到爆出了 flag：