0x00 前言

有技术交流或渗透测试培训需求的朋友欢迎联系QQ/VX-547006660，

需要代码审计、渗透测试、红蓝对抗网络安全相关业务可以联系我司

2000人网络安全交流群，欢迎大佬们来交流 群号820783253

最近BugBounty挖了不少，但大多数都是有手就行的漏洞，需要动脑子的实属罕见

而今天就遇到了一个非常好的案例，故作此文

0x01 对目录批量FUZZ，发现一处隐蔽接口

挖某大厂已经挖了快两个周了，期间因为公司业务比较繁忙，最近一直没挖。

但是一直在用ffuf挂着字典对厂商资产进行批量目录扫描，今天上服务器看了下扫描结果，就出货了

接口地址为：https://xxx.xxxx.com/xxxx/start

我们直接对其进行访问

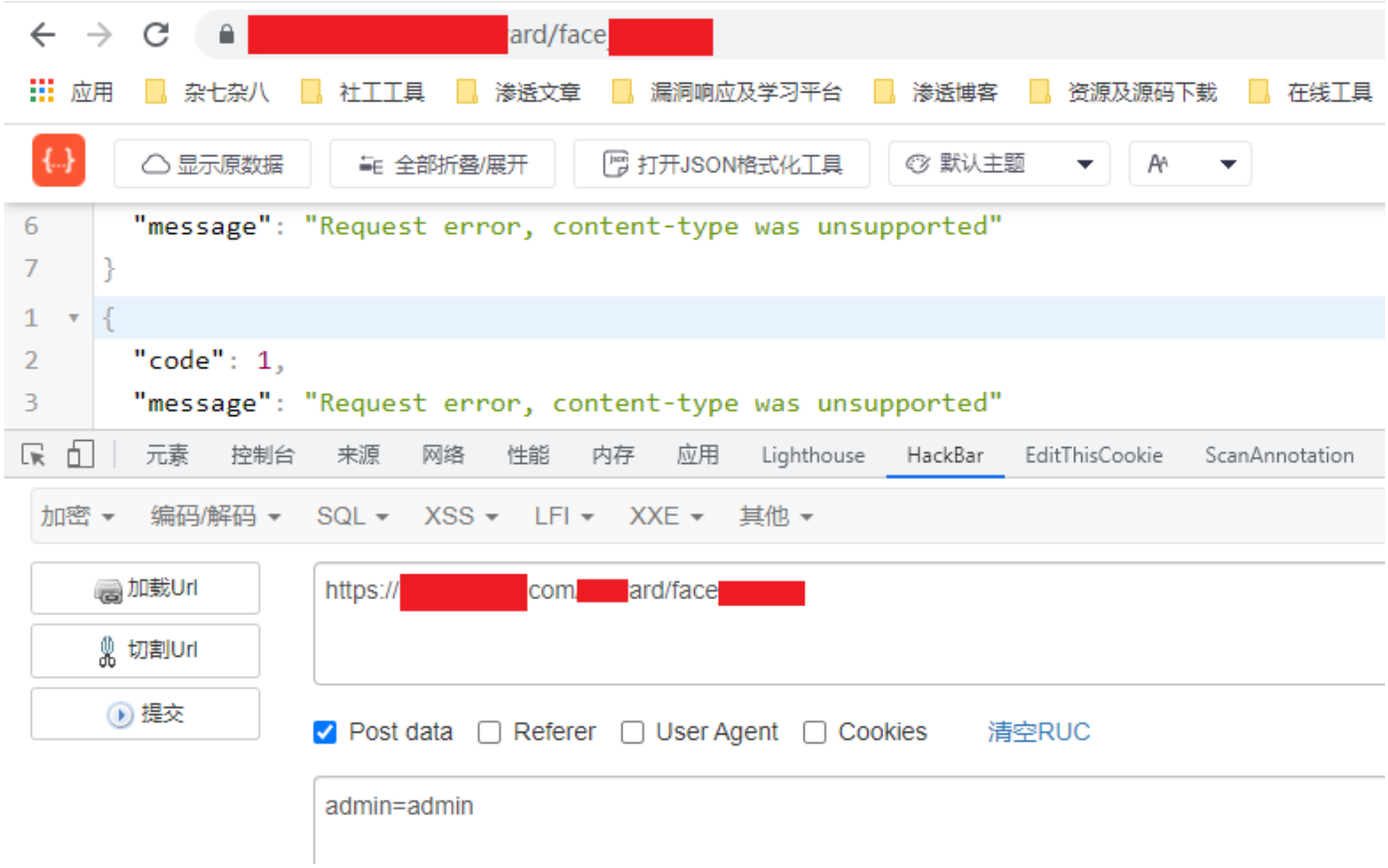
发现该接口给我们提供了一些可以使用的接口链接

我们逐个测试拼接接口后，发现一个名为face_xxxx的接口有戏

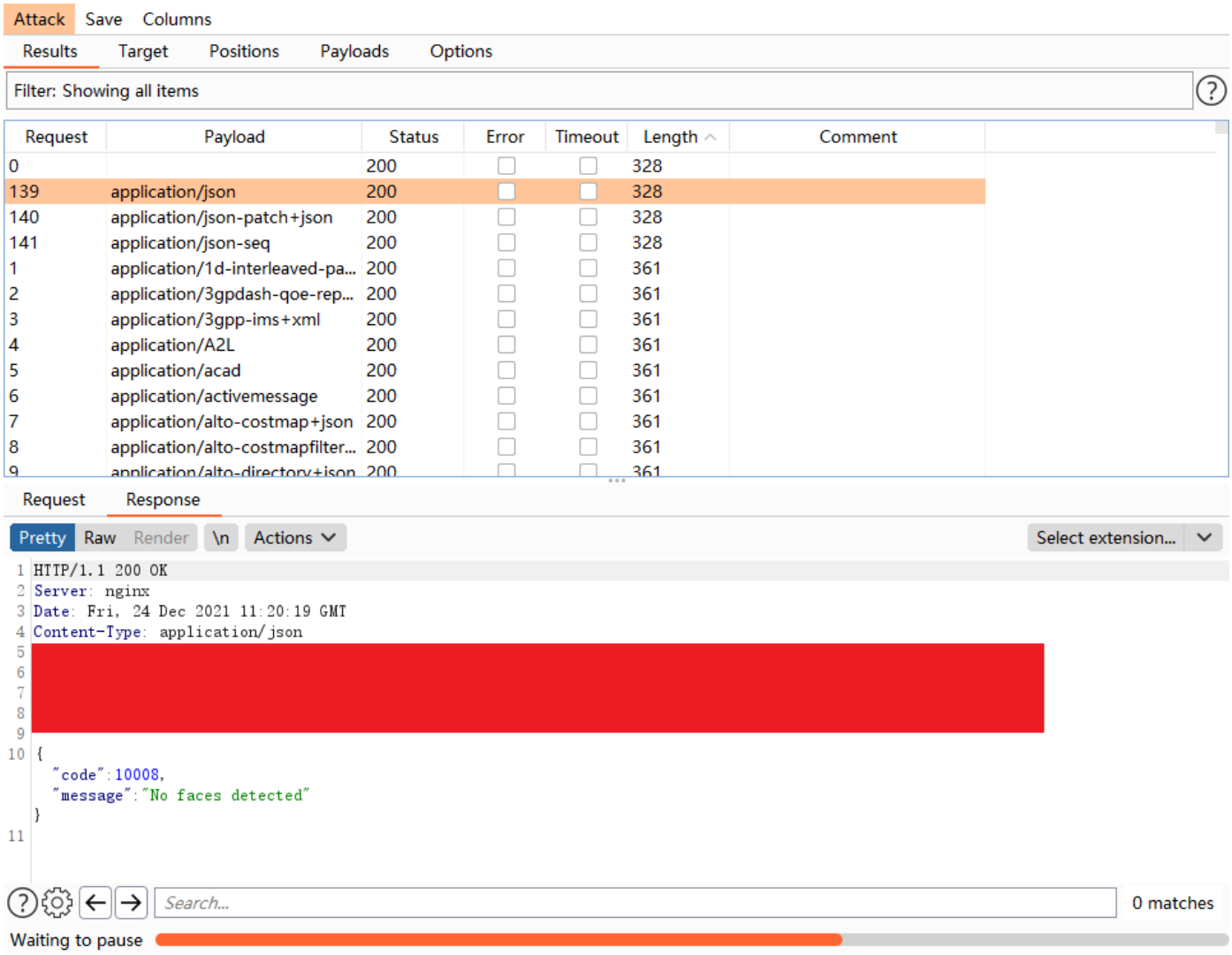
0x02 FUZZ传参格式+参数

访问接口，提示Method Not Allow，405错误，那么很显然，我们得换POST传参

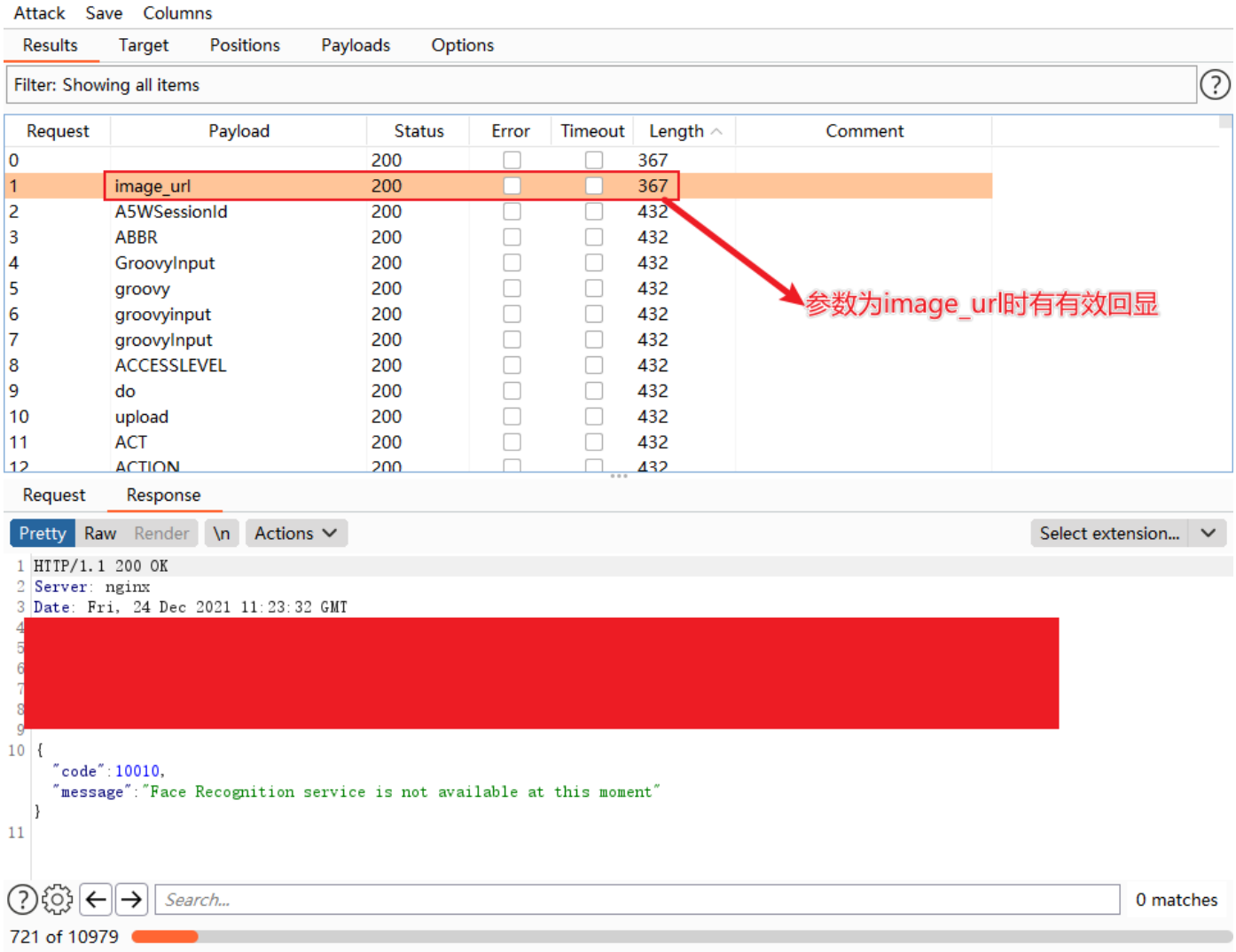
POST随便传个参过去，发现接口提示"Request error, content-type was unsupported"



很好，继续FUZZ content-type header(记得把payload_processing自动编码给关掉)



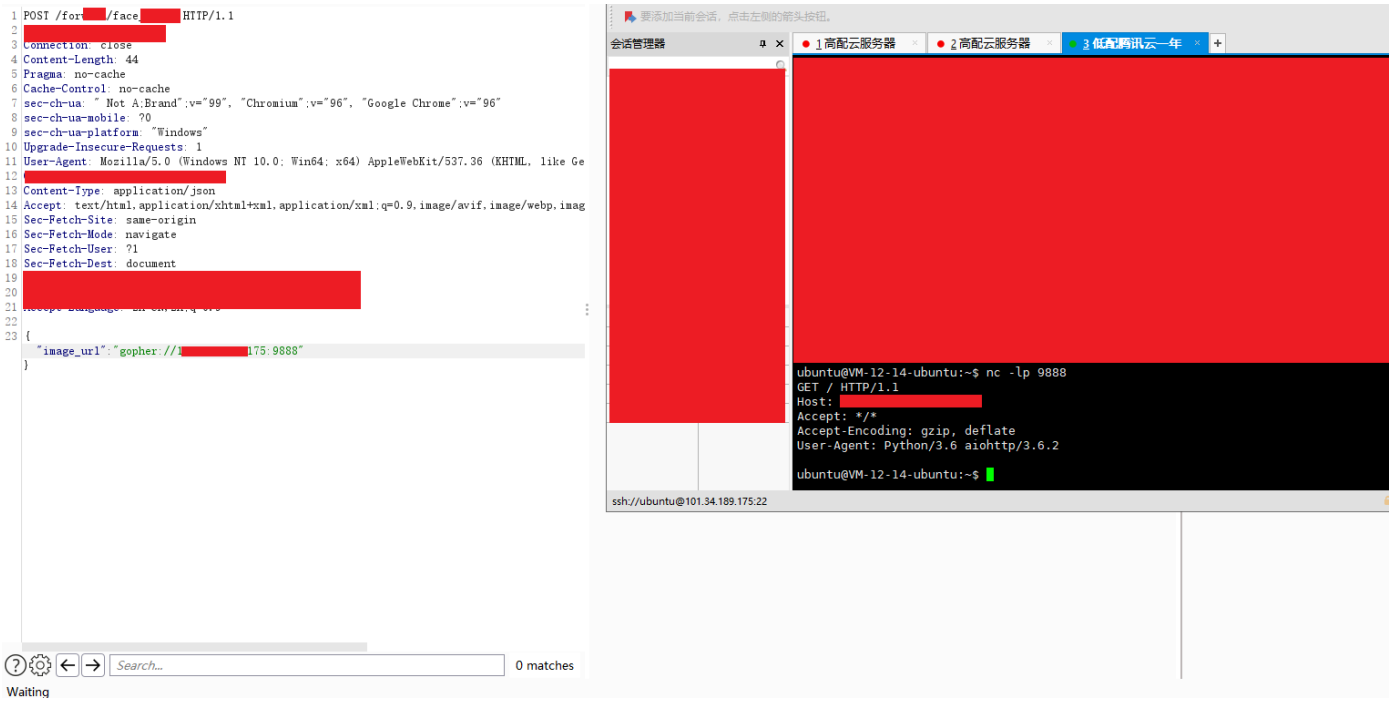
FUZZ出来application/json的content-type头可用，那么很简单了，构造JSON数据，继续FUZZ JSON数据参数



0x03 SSRF无脑到手

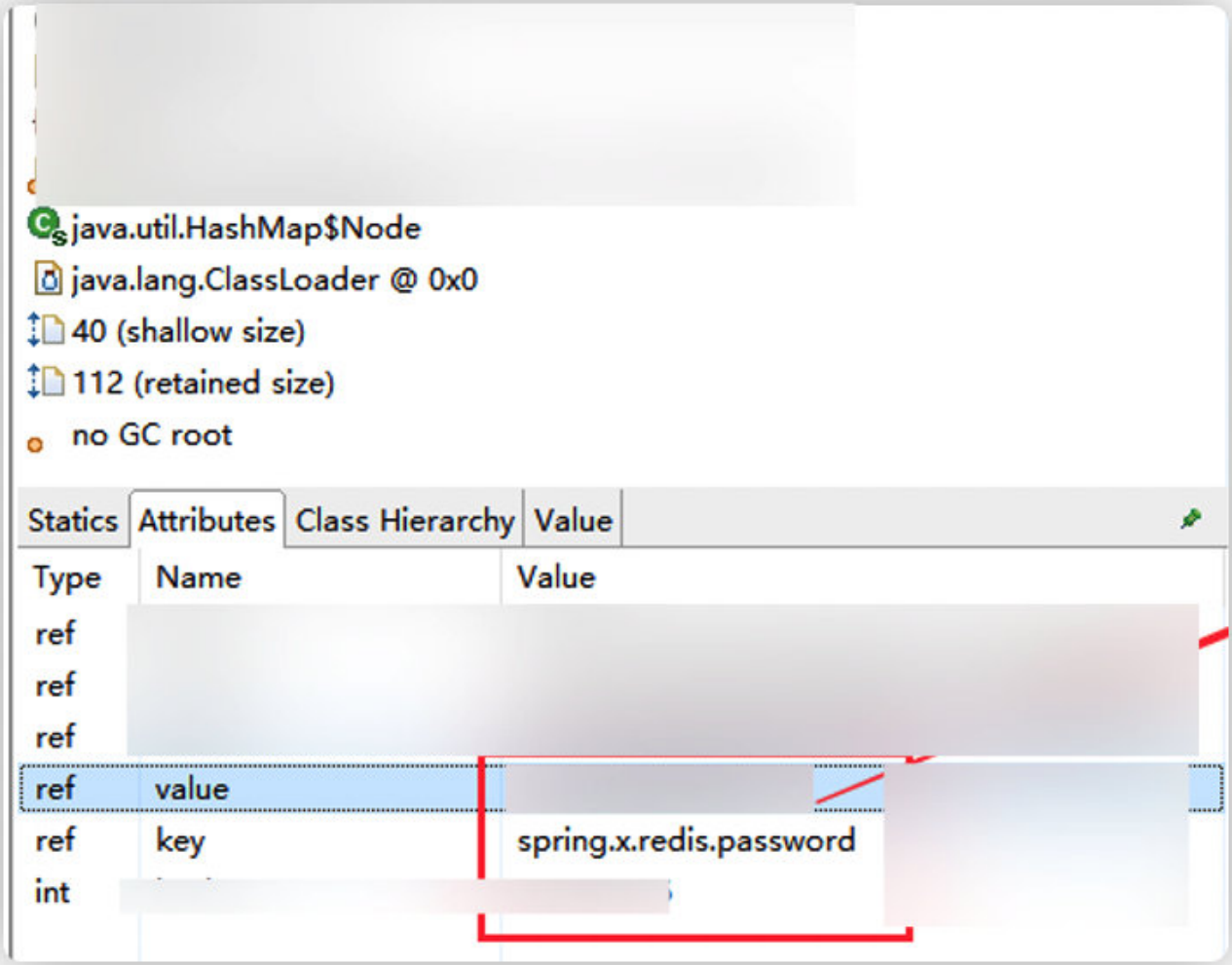
参数为image_url，稍有经验的朋友就可以借此判断出，很可能这个参数是加载远程图片的

直接进行SSRF测试



服务器收到了请求，经测试gopher，dict，http等常规协议都可以使用~

之前通过各种域名二级目录或根目录的spring泄露，下载heapdump，OQL调试出redis明文密码



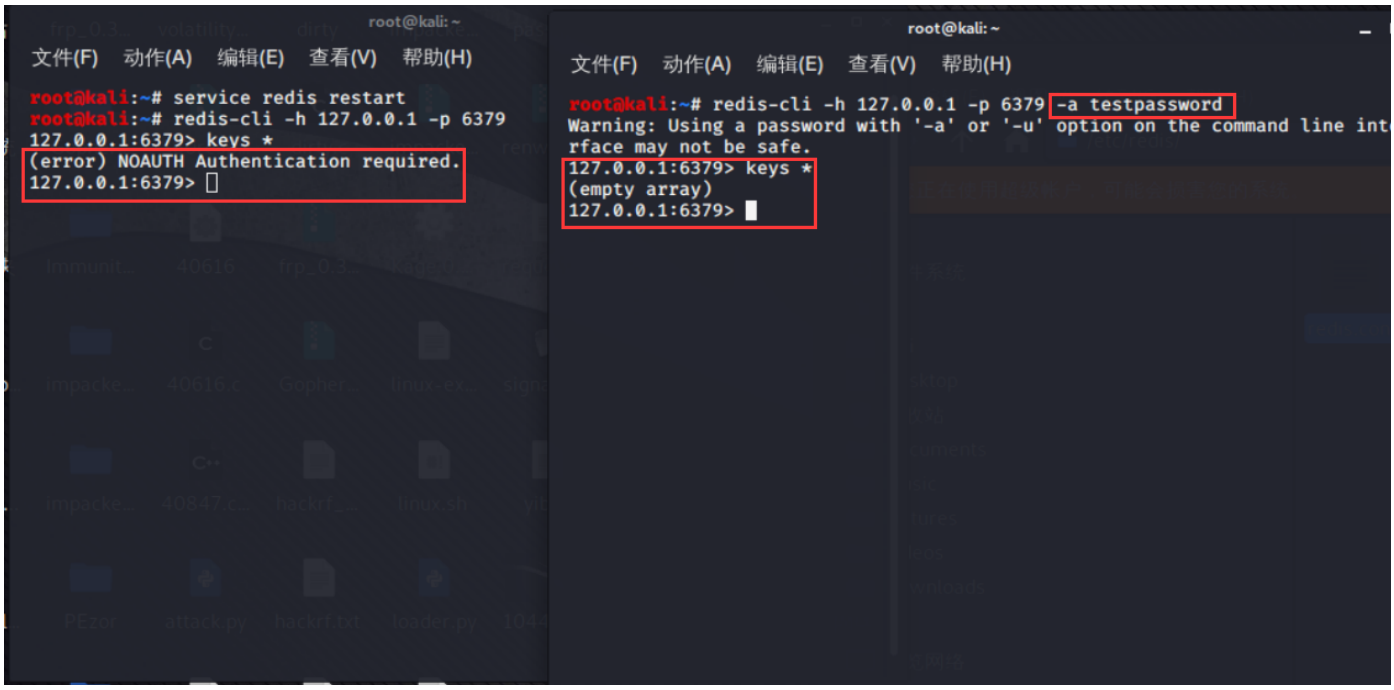
收集了不少该厂商内网redis的ip和密码，也了解到该厂商的内网网段

尝试利用本处SSRF完全可以批量对内网Redis进行密码喷洒+反弹shell对边界进行突破

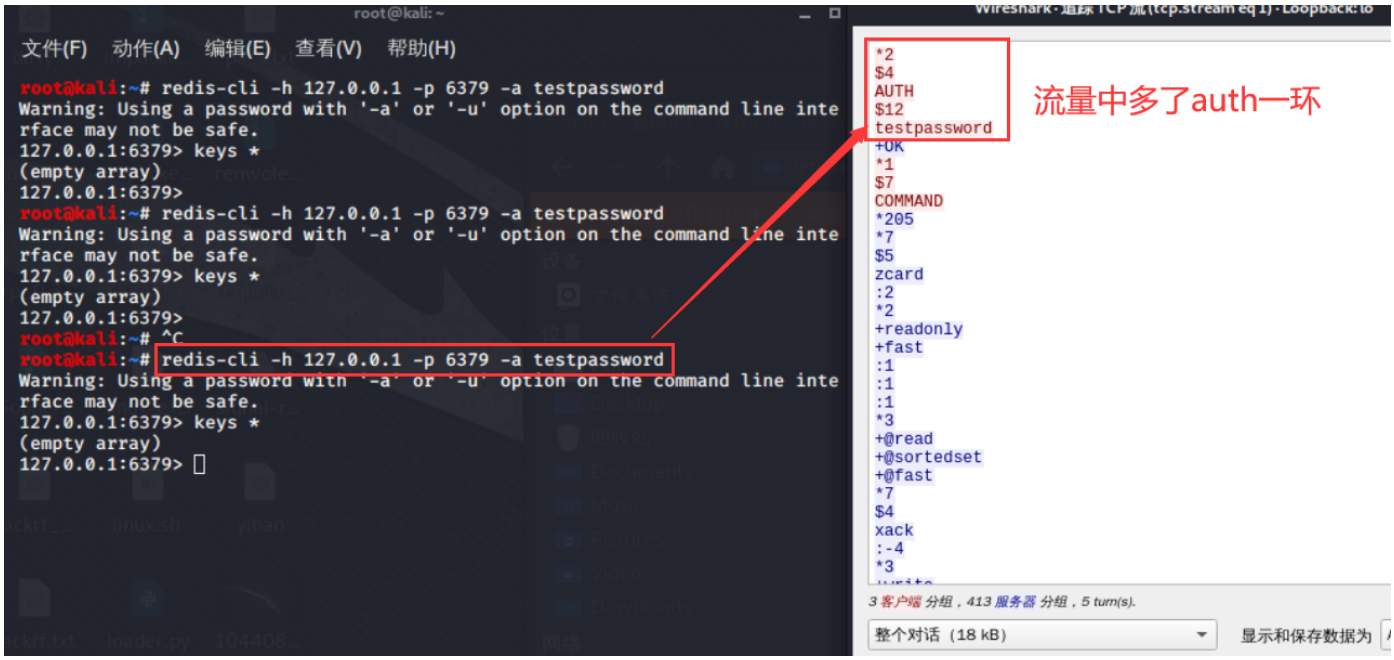
0x04 利用gopher协议对内网脆弱网段批量Redis密码喷洒反弹Shell

普及一个知识：与未授权直接访问的redis不同，加入密码认证的redis在命令行链接时会多一个-a参数指定密码

如图所示如果不传参密码，则无法执行任何redis指令

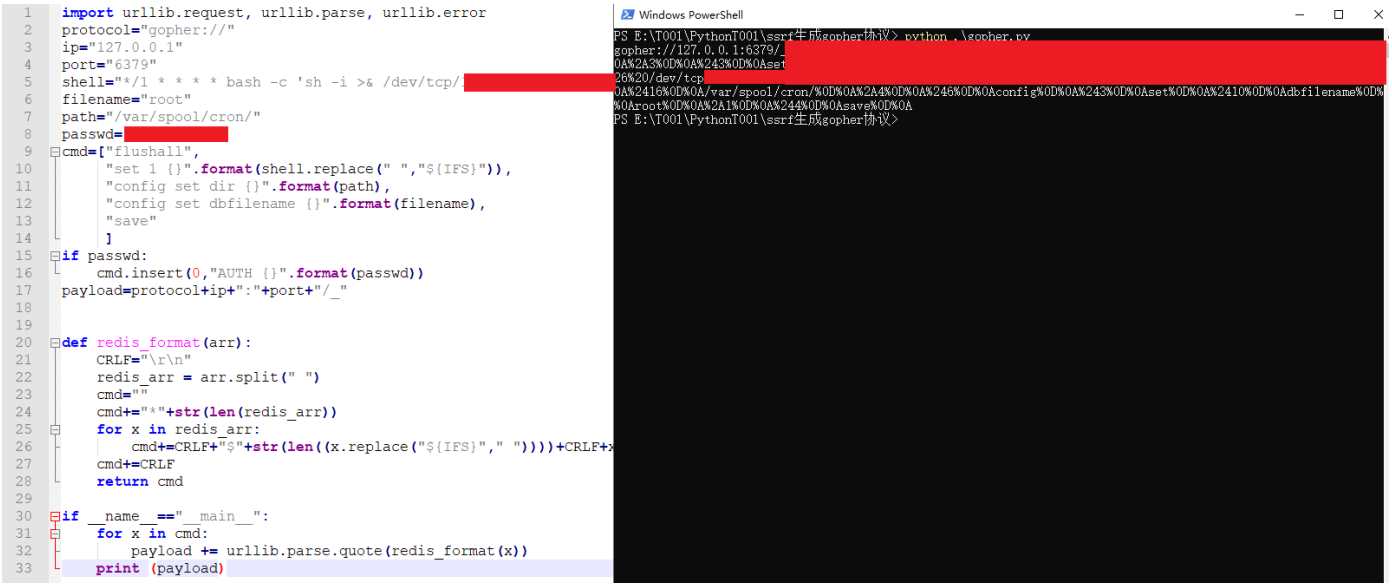


而加入密码认证后redis，在整个RESQ协议流量中表现如下



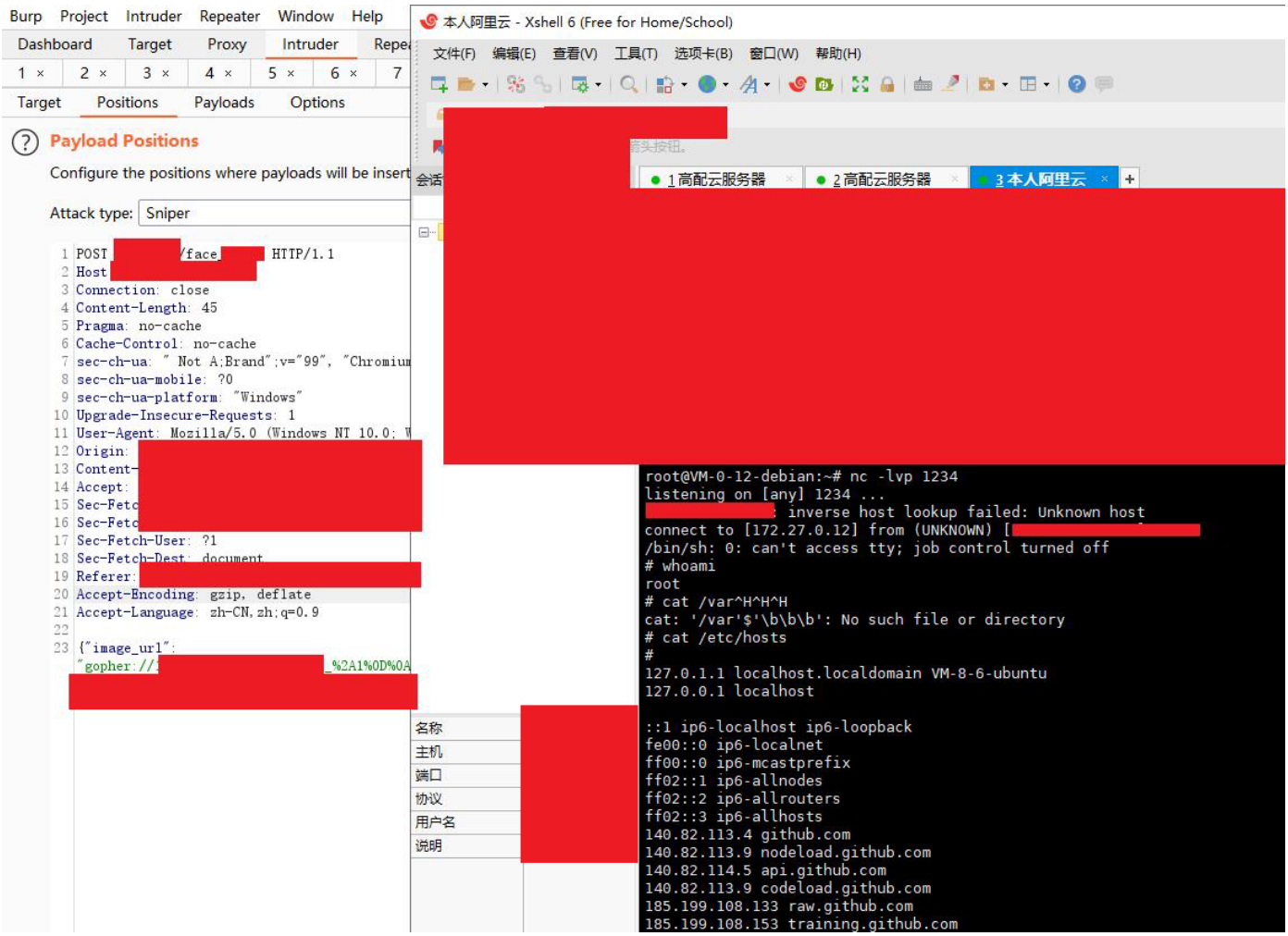
认证过程中会多一个Auth

写脚本来构造gopher数据，注意把这块Auth加上,后续常规操作写计划任务反弹SHELL



利用上面挖掘到的SSRF点，配合之前自己收集到的内网redis密码和脆弱网段

直接通过intruder批量跑内网的脆弱网段redis，进行密码喷洒，喷洒一但成功，则会写入计划任务



最终功夫不负有心人，在一个网段，弹回来了十几个Shell。。。

厂商的内网Redis主机还能出网，属实是内网安全做的稀烂了。

```
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# ls
# ls-^H
/bin/sh: 3: ls: not found
# w
 00:05:12 up 166 days,  7:21,  0 users,  load average: 2.86, 2.77, 2.69
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
# ls -lah
total 44K
drwx------  7 root   root   4.0K Aug 25 19:19 .
drwxr-xr-x 31 root   root   4.0K Dec 25 00:05 ..
-rw-------  1 root   root      2 May  7  2021 .bash_history
-rw-r--r--  1 ubuntu ubuntu 3.2K Jul  1 16:06 .bashrc
drwx------  2 root   root   4.0K Aug  9  2018 .cache
drwx------  3 root   root   4.0K Aug  9  2018 .gnupg
drwxr-xr-x  3 root   root   4.0K Aug 25 19:19 .local
drwxr-xr-x  2 root   root   4.0K May  7  2021 .pip
-rw-r--r--  1 root   root    148 Aug 17  2015 .profile
-rw-r--r--  1 root   root     73 May  7  2021 .pydistutils.cfg
drwx------  2 root   root   4.0K May 29  2019 .ssh
-rw-------  1 root   root      0 May  7  2021 .viminfo
# cd ../
```

0x04 后言

这个洞是在平安夜挖到的~算是圣诞贺礼啦