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

0x01 起因

朋友给某甲方做渗透测试，奈何甲方是某知名保险，系统太耐艹，半天不出货

兄弟喊我来一块来看，于是有了本文

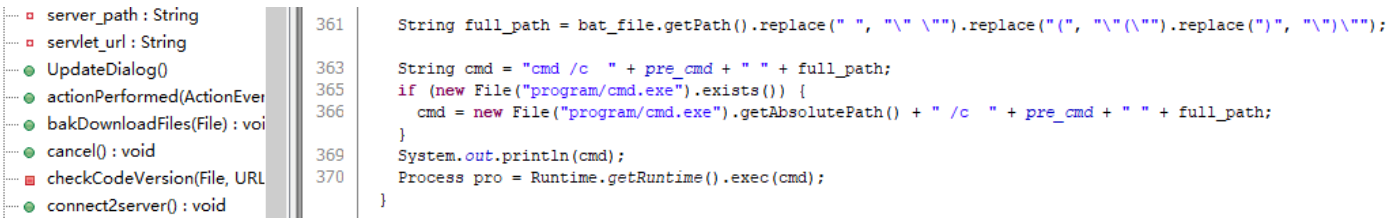
0x02 客户端RCE一处

朋友把靶标发给我看了下，除了两个下载链接啥也没有

链接下载下来的东西如图，看了下目录里面还有JRE，那么很显然，这客户端exe就是个JAVA启动命令执行套壳

随后打开program文件夹，逆了一下里面的Jar

full_path前面定义为用户更新时输入的路径



那么很简单了full_path可控，诱导用户安装更新时路径出输入注入命令即可

```
D:\software  && ping hacker's IP
```

Get SubDomain | Refresh Record

l6sxhv.dnslog.cn

DNS Query Record	[redacted]	Created Time
l6sxhv.dnslog.cn		2021-12-21 16:44:58
l6sxhv.dnslog.cn		2021-12-21 16:44:57
l6sxhv.dnslog.cn		2021-12-21 16:44:57
l6sxhv.dnslog.cn		2021-12-21 16:44:57

0x03 发现Webservice Soap接口

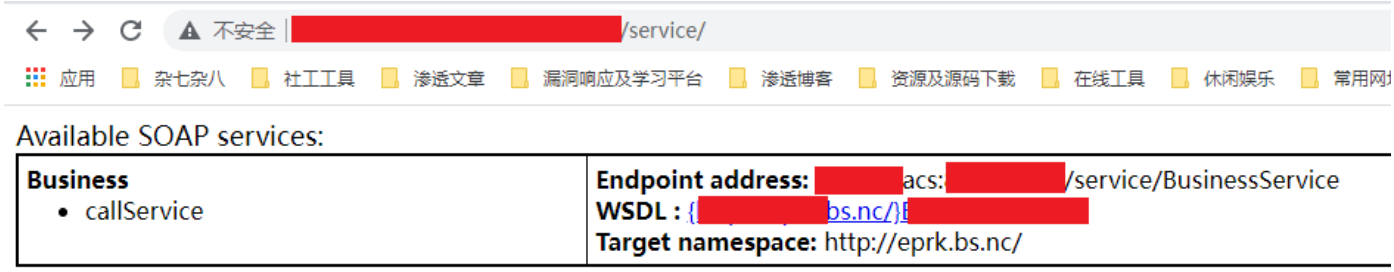
光这一个水来的客户端RCE肯定是不够的，接下来继续挖掘服务端

看了看没别的功能点，我就简单FUZZ了一下这个系统三级目录

```
ubuntu@VM-8-6-ubuntu:~/ffuf$ ./ffuf -w content.txt -u http://[redacted]/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1
________________________________________________

 :: Method           : GET
 :: URL              : http://[redacted]/FUZZ
 :: Wordlist         : FUZZ: content.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________
```

最后FUZZ出来了一个webservice接口

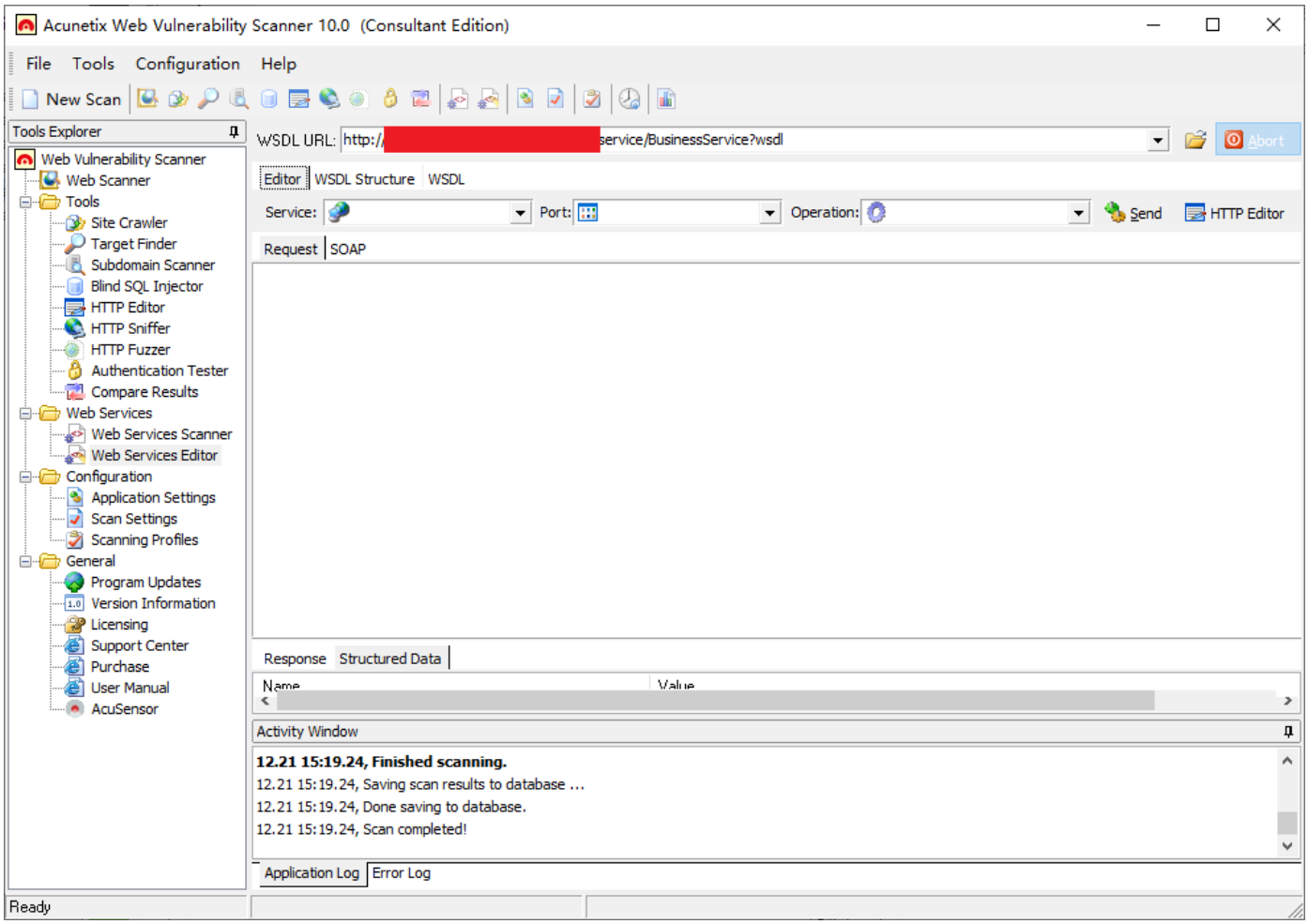
http://.xxxxxx.cn/xxxx/service



拼接出其wsdl接口

http://.xxxxxx.cn/xxxx/service/BusinessService?wsdl

但导入SoapUI或AWVS的调试模块进行调试时却发现其导入失败



仔细看了下WSDL返回的信息。。。妈的WSDL Import Location和Soap Address Location都是内网域名

不过幸运的是，该系统的外网域名拼接路径后也可以访问到这个WSDL接口

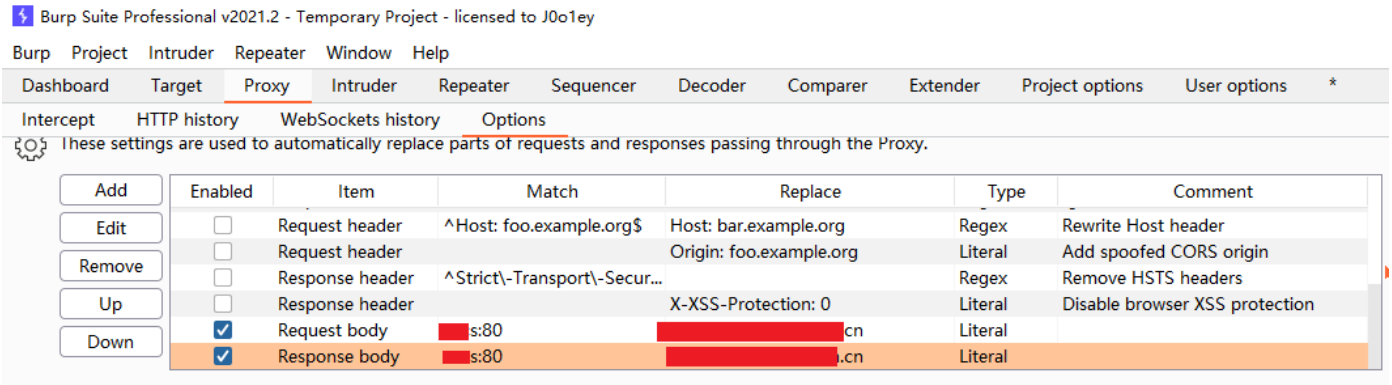
但是自动化的Soap接口调试工具是“看见什么就import什么”，这可让人犯了难

0x04导入SoapUI

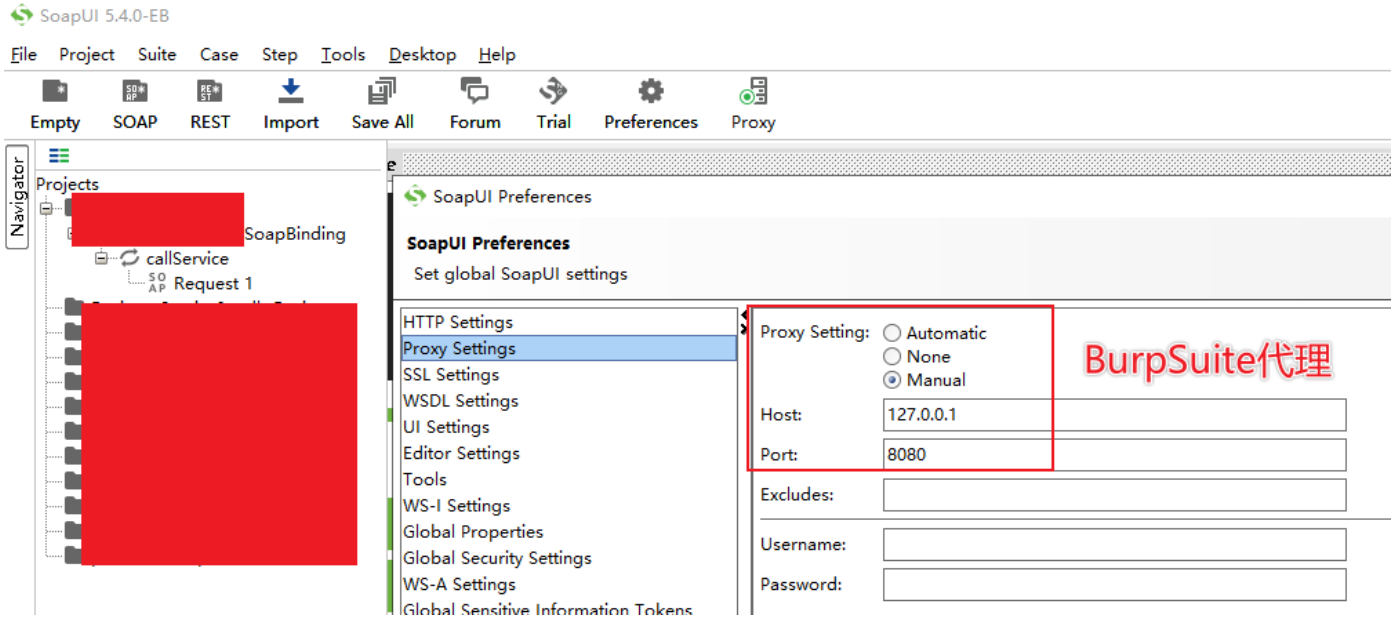
思考了一会，突然想起来BurpSuite可以把RequestBody和ResponseBody的值进行替换，hhh，那我们就有办法导入了

在Burpsuite的Porxy Option中增加Match&Replace规则

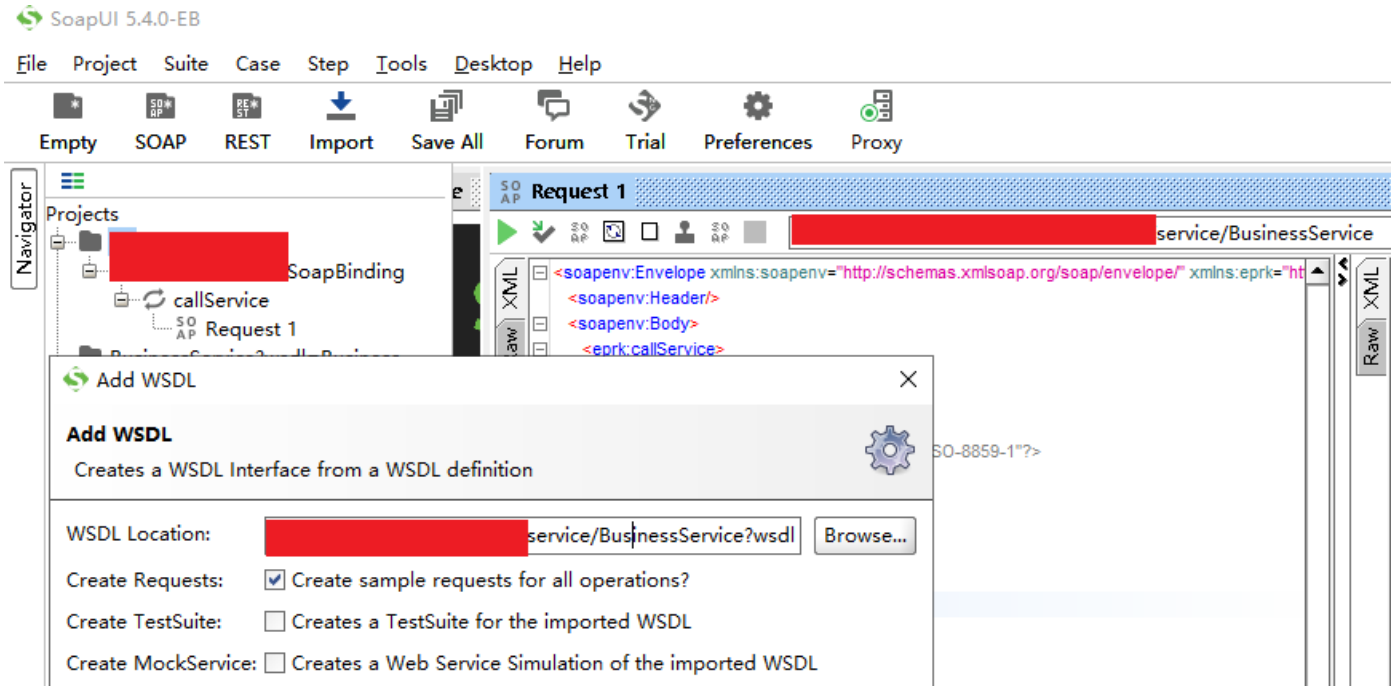
将WSDL Import Location和Soap Address Location处对应的内网域名都替换为外网域名



随后在SoapUI中设置Proxy

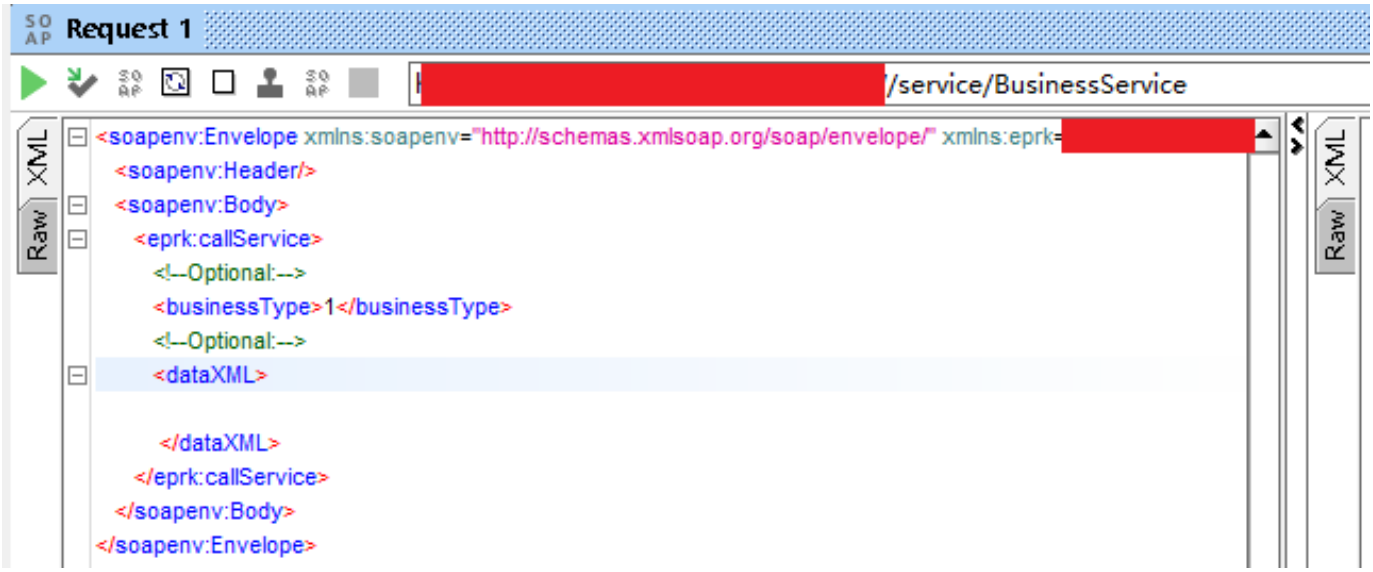


打开代理，再次添加WSDL，ResponseBody的内网域名成功被替换，WSDL导入成功~



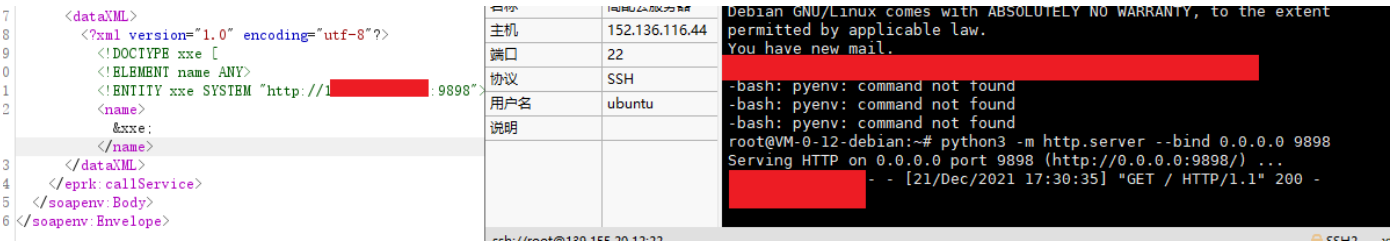
0x05 XXE挖掘

导入接口后，发现有参数为dataXML，心中暗喜XXE估计是送上门了



直接BurpSuite中利用XXE OOB测试

OOB成功，XXE到手，收摊~



0x06 总结

坚持一下，守得云开见月明，漏洞就在眼前~