BUUCTF 真的很杂

原创

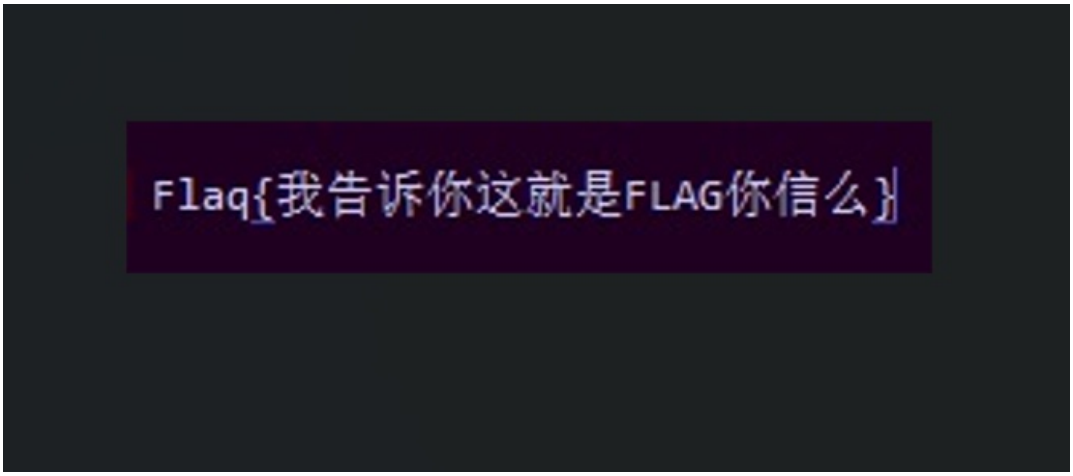
cuihua2021 于 2022-04-03 20:18:19 发布 190 收藏

分类专栏： BUU-Misc 文章标签： 其他

本文链接：https://blog.csdn.net/WYHPROGRAME/article/details/123943424

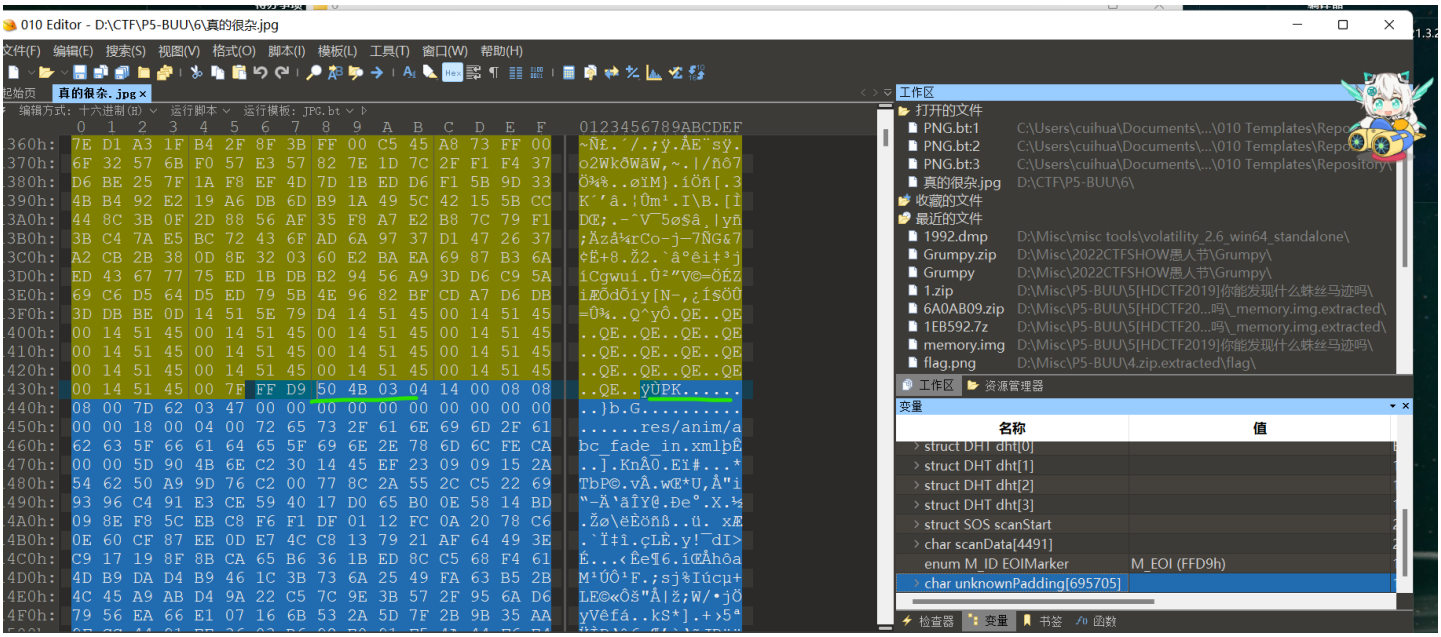
真的很杂

1.题目概述

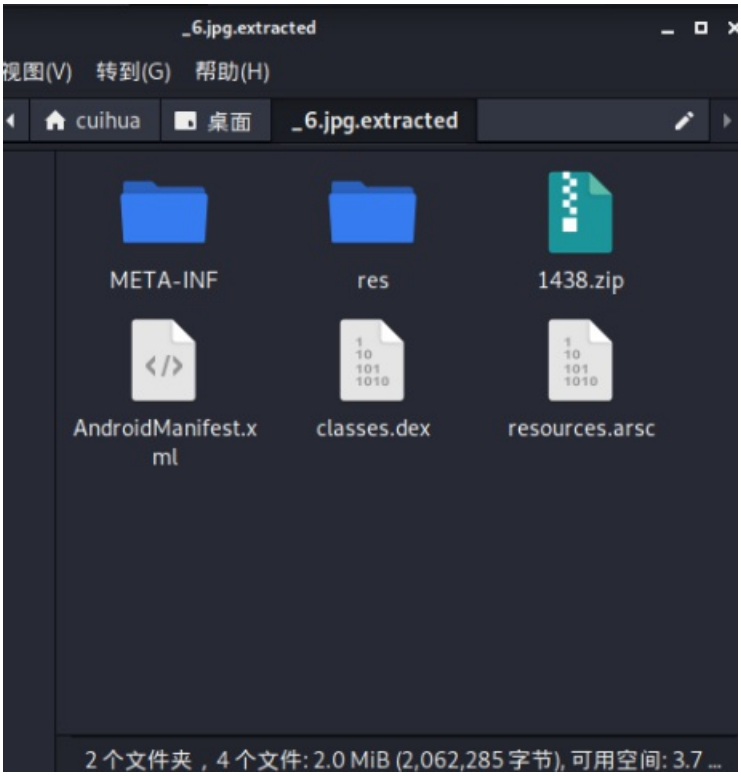


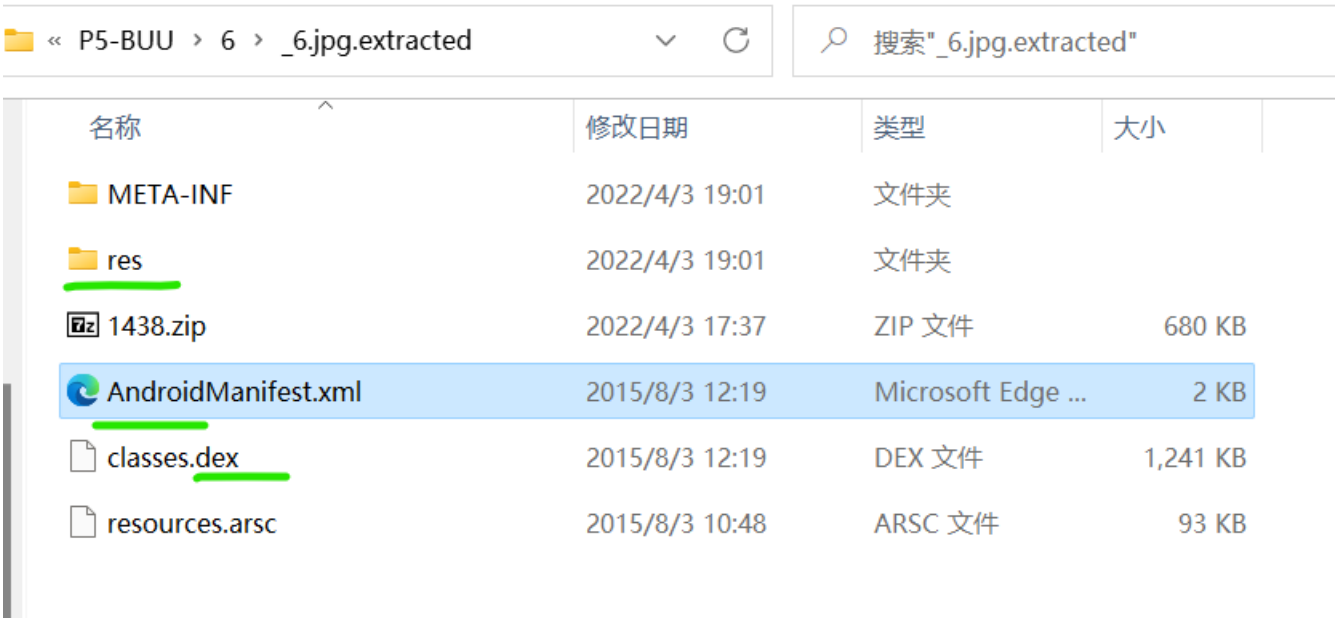
2.解题过程

只有一张图片，010打开



结尾发现zip，binwalk分离（foremost分离出一堆没用的照片）





准备安卓逆向工具

1.apktool——可以反编译软件的布局文件、图片等资源，方便大家学习一些很好的布局；
2.dex2jar——将apk反编译成java源码（classes.dex转化成jar文件）；
3.jd-gui——查看APK中classes.dex转化成出的jar文件，即源码文件。

apktool（选最新版

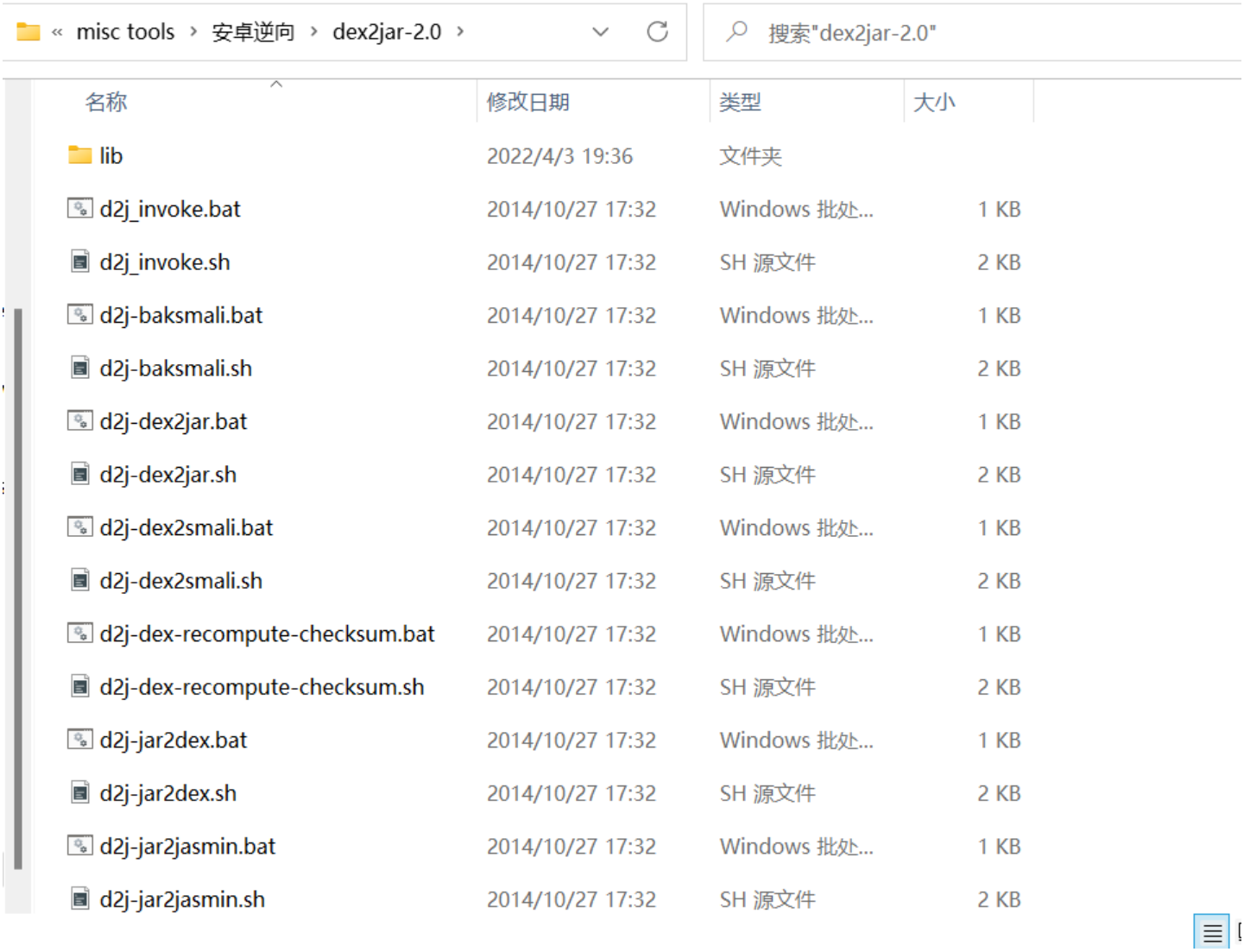
iBotPeaches / Apktool / Downloads — Bitbucket
然后把这个网址里的东西复制粘贴保存为apktool.bat,和上面下载的apktool.jar放在同一个目录下

https://raw.githubusercontent.com/iBotPeaches/Apktool/master/scripts/windows/apktool.bat

apktool.dat	2022/4/3 19:22	DAT 文件	2 KB
apktool_2.6.1.jar	2022/4/3 19:21	Executable Jar ...	19,514 KB

安装工具dex2jar2.0

Download dex2jar from SourceForge.net



misc tools › 安卓逆向 › dex2jar-2.0 ›

搜索"dex2jar-2.0"

名称	修改日期	类型	大小
lib	2022/4/3 19:36	文件夹	
d2j_invoke.bat	2014/10/27 17:32	Windows 批处...	1 KB
d2j_invoke.sh	2014/10/27 17:32	SH 源文件	2 KB
d2j-baksmali.bat	2014/10/27 17:32	Windows 批处...	1 KB
d2j-baksmali.sh	2014/10/27 17:32	SH 源文件	2 KB
d2j-dex2jar.bat	2014/10/27 17:32	Windows 批处...	1 KB
d2j-dex2jar.sh	2014/10/27 17:32	SH 源文件	2 KB
d2j-dex2smali.bat	2014/10/27 17:32	Windows 批处...	1 KB
d2j-dex2smali.sh	2014/10/27 17:32	SH 源文件	2 KB
d2j-dex-recompute-checksum.bat	2014/10/27 17:32	Windows 批处...	1 KB
d2j-dex-recompute-checksum.sh	2014/10/27 17:32	SH 源文件	2 KB
d2j-jar2dex.bat	2014/10/27 17:32	Windows 批处...	1 KB
d2j-jar2dex.sh	2014/10/27 17:32	SH 源文件	2 KB
d2j-jar2jasmin.bat	2014/10/27 17:32	Windows 批处...	1 KB
d2j-jar2jasmin.sh	2014/10/27 17:32	SH 源文件	2 KB

下载jd-gui(我下载的win版)

程序：

Java Decompiler (java-decompiler.github.io)

jar文件

java-decompiler/jd-gui: A standalone Java Decompiler GUI (github.com)

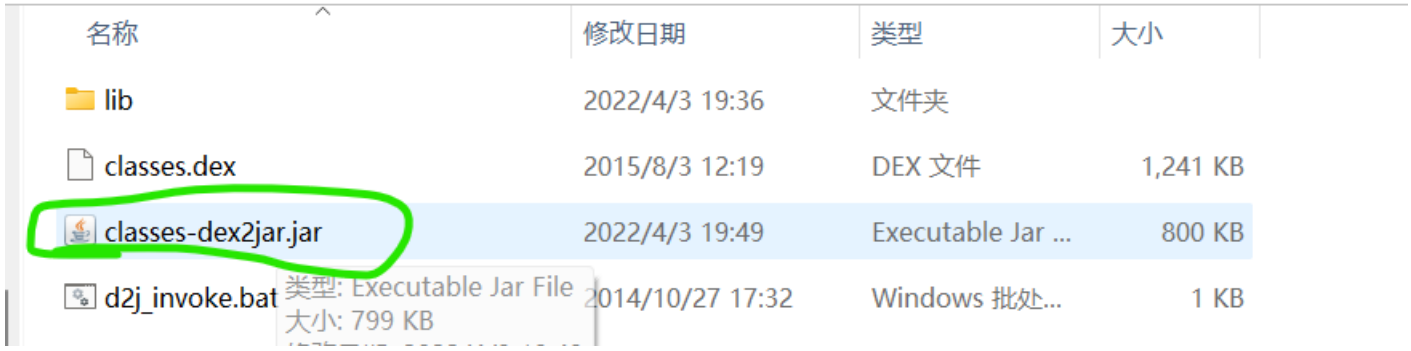
开干

把class.dex文件放到dex2jar目录下，打开终端，输入

```
./d2j-dex2jar.bat classes.dex
```

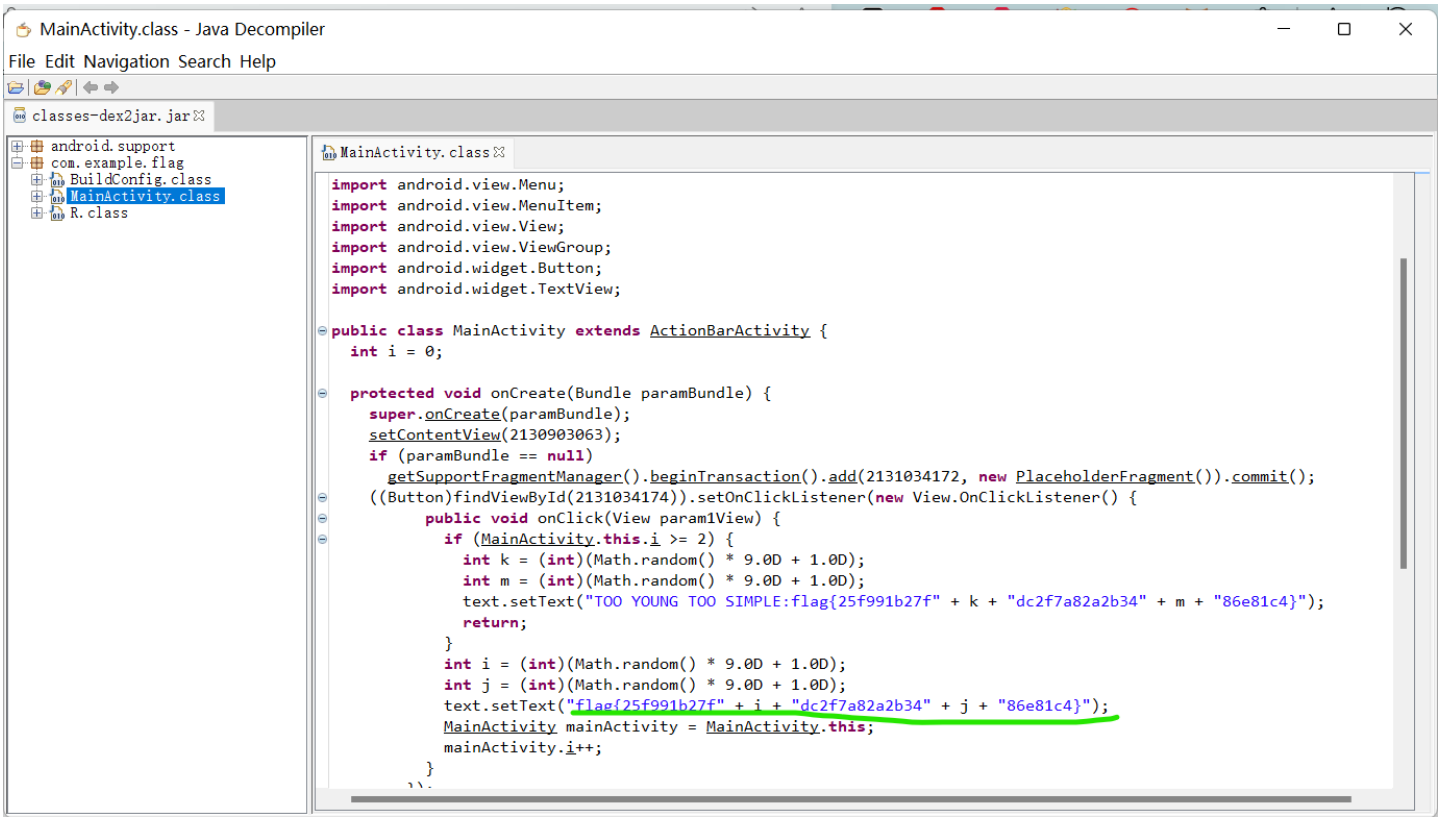
```
PS D:\CTF\misc tools\安卓逆向\dex2jar-2.0> ./d2j-dex2jar.bat classes.dex
dex2jar classes.dex -> .\classes-dex2jar.jar
java.nio.file.NoSuchFileException: classes.dex
        at sun.nio.fs.WindowsException.translateToIOException(Unknown Source)
        at sun.nio.fs.WindowsException.rethrowAsIOException(Unknown Source)
        at sun.nio.fs.WindowsException.rethrowAsIOException(Unknown Source)
        at sun.nio.fs.WindowsFileSystemProvider.newByteChannel(Unknown Source)
        at java.nio.file.Files.newByteChannel(Unknown Source)
        at java.nio.file.Files.newByteChannel(Unknown Source)
        at java.nio.file.Files.readAllBytes(Unknown Source)
        at com.googlecode.d2j.reader.zip.ZipUtil.readDex(ZipUtil.java:57)
        at com.googlecode.d2j.reader.zip.ZipUtil.readDex(ZipUtil.java:53)
        at com.googlecode.dex2jar.tools.Dex2jarCmd.doCommandLine(Dex2jarCmd.java:104)
        at com.googlecode.dex2jar.tools.BaseCmd.doMain(BaseCmd.java:288)
        at com.googlecode.dex2jar.tools.Dex2jarCmd.main(Dex2jarCmd.java:32)
PS D:\CTF\misc tools\安卓逆向\dex2jar-2.0>
```

然后会生成一个jar文件



或者直接把class.dex文件拖到d2j-dex2jar.bat上面，也能生成这个文件

然后把这个jar文件用jd-gui.exe打开



不难看到flag(我近视都能发现，你不会看不到吧？)

```
flag{25f991b27f" + i + "dc2f7a82a2b34" + j + "86e81c4}
```

i和j代表题目中要我们爆破的字母和数字

多试几十次之后，得到flag

flag{25f991b27fcdc2f7a82a2b34386e81c4}

3.flag

flag{25f991b27fcdc2f7a82a2b34386e81c4}