

# 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/WYHPROGRAMME/article/details/123943424>

版权



[BUU-Misc 专栏收录该内容](#)

9 篇文章 0 订阅

订阅专栏

## 真的很杂

### 1. 题目概述

题目

解题快手榜



# 真的很杂

## 1

杂项题目经常混杂着奇奇怪怪的东西。。。不要想歪了! 专心做题==! 最后获得的东西需要暴力得到哦 (提示: 前一个字母, 后一个数字) 注意: 得到的flag 请包上 flag{} 提交

2d883323-9...

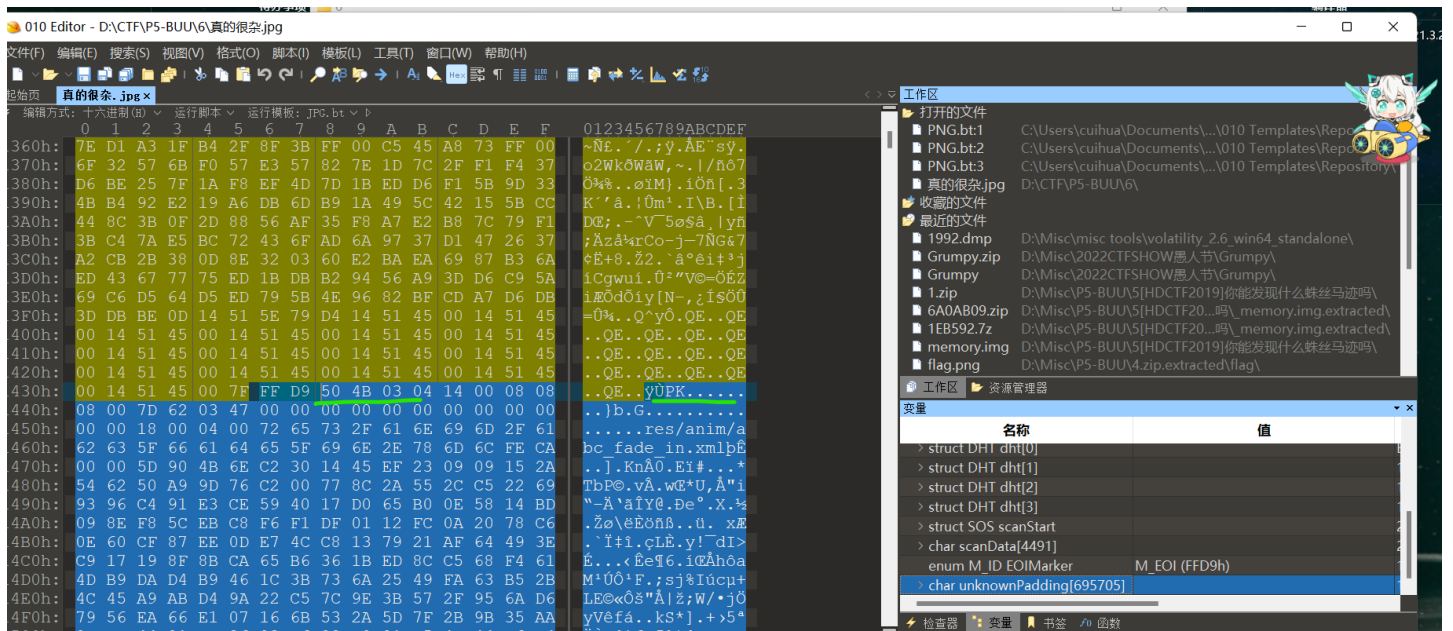
Flag

提交

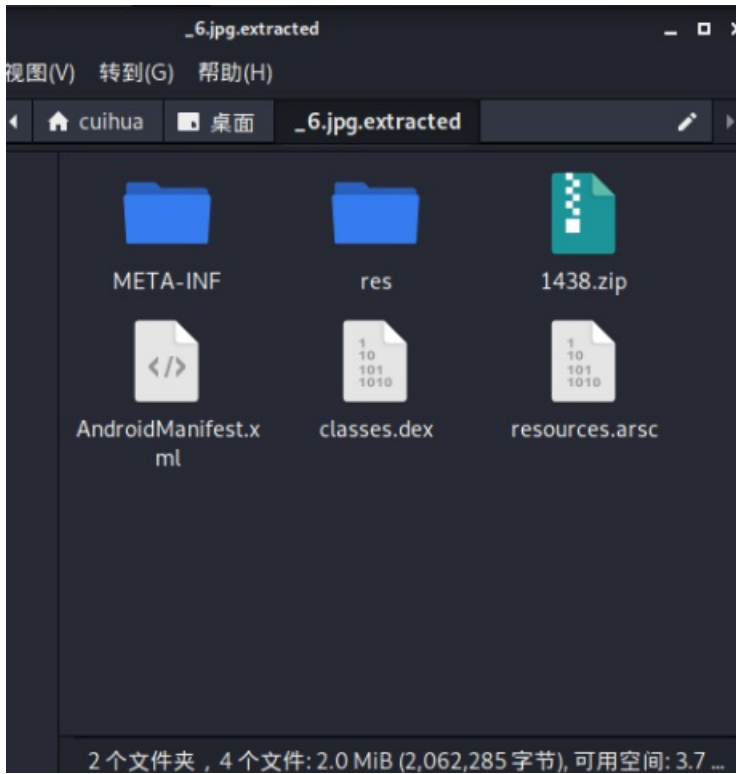
Flag{我告诉你这就是FLAG你信么}

## 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)



名称	修改日期	类型	大小
META-INF	2022/4/3 19:01	文件夹	
res	2022/4/3 19:01	文件夹	
1438.zip	2022/4/3 17:37	ZIP 文件	680 KB
AndroidManifest.xml	2015/8/3 12:19	Microsoft Edge ...	2 KB
classes.dex	2015/8/3 12:19	DEX 文件	1,241 KB
resources.arsc	2015/8/3 10:48	ARSC 文件	93 KB

## 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](#)

名称	修改日期	类型	大小
misc tools > 安卓逆向 > dex2jar-2.0			
搜索"dex2jar-2.0"			
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 \(github.com\)](#)

jd-gui-master	2022/4/3 19:27	文件夹
jd-gui-windows-1.6.6	2022/4/3 19:52	文件夹

## 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.io.File.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

名称	修改日期	类型	大小
lib	2022/4/3 19:36	文件夹	
classes.dex	2015/8/3 12:19	DEX 文件	1,241 KB
classes-dex2jar.jar	2022/4/3 19:49	Executable Jar ...	800 KB
d2j_invoke.bat	2014/10/27 17:32	Windows 批处...	1 KB

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

```
MainActivity.class - Java Decompiler
File Edit Navigation Search Help
classes-dex2jar.jar
  android.support
  com.example.flag
  BuildConfig.class
  MainActivity.class
  R.class
MainActivity.class
import android.view.Menu;
import android.view.MenuItem;
import android.view.View;
import android.view.ViewGroup;
import android.widget.Button;
import android.widget.TextView;

public class MainActivity extends ActionBarActivity {
    int i = 0;

    protected void onCreate(Bundle paramBundle) {
        super.onCreate(paramBundle);
        setContentView(2130903063);
        if (paramBundle == null)
            getSupportFragmentManager().beginTransaction().add(2131034172, new PlaceholderFragment()).commit();
        ((Button)findViewById(2131034174)).setOnClickListener(new View.OnClickListener() {
            public void onClick(View param1View) {
                if (MainActivity.this.i >= 2) {
                    int k = (int)(Math.random() * 9.0D + 1.0D);
                    int m = (int)(Math.random() * 9.0D + 1.0D);
                    text.setText("TOO YOUNG TOO SIMPLE:flag{25f991b27f" + k + "dc2f7a82a2b34" + m + "86e81c4}");
                    return;
                }
                int i = (int)(Math.random() * 9.0D + 1.0D);
                int j = (int)(Math.random() * 9.0D + 1.0D);
                text.setText("flag{25f991b27f" + i + "dc2f7a82a2b34" + j + "86e81c4}");
                MainActivity mainActivity = MainActivity.this;
                mainActivity.i++;
            }
        });
    }
}
```

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}
```