

BUUCTF 真的很杂

原创

wangjin7356 已于 2022-03-08 10:15:54 修改 92 收藏 1

分类专栏: [CTF](#) 文章标签: [安全](#)

于 2022-03-08 10:13:57 首次发布

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/wangjin7356/article/details/123345899>

版权



[CTF 专栏收录该内容](#)

49 篇文章 0 订阅

订阅专栏

题目链接

<https://buuoj.cn/challenges/#%E7%9C%9F%E7%9A%84%E5%BE%88%E6%9D%82>

解题过程

题目 [解题快手榜](#) ×

真的很杂

1

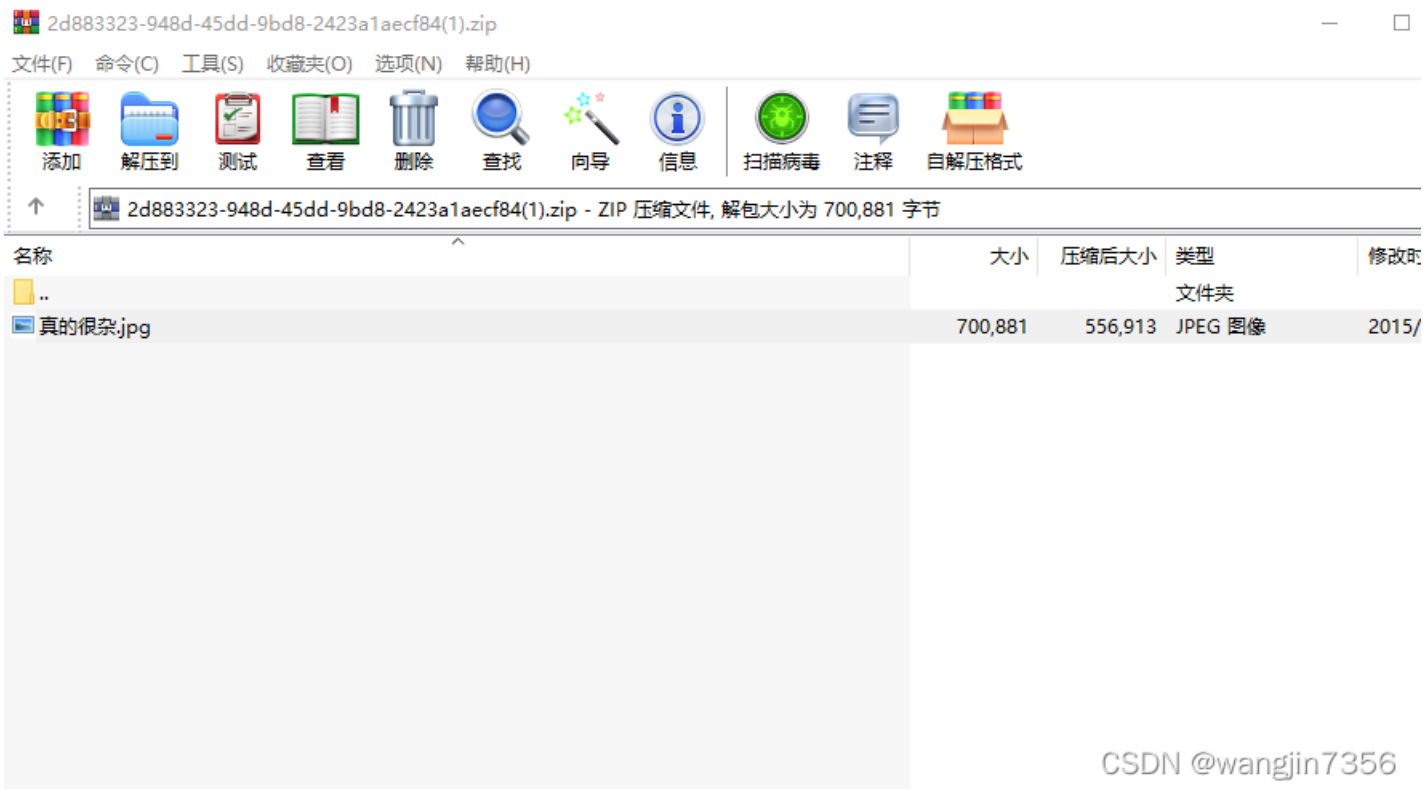
杂项题目经常混杂着奇奇怪怪的东西。。。不要想歪了! 专心做题 = =! 最后获得的东西需要暴力得到哦 (提示: 前一个字母, 后一个数字) 注意: 得到的 flag 请包上 flag{} 提交

[2d883323-9...](#)

Flag

CSDN @wangjin7356

题目是张图片:



CSDN @wangjin7356

Flaq{我告诉你这就是FLAG你信么}

使用binwalk工具，得到安卓的应用

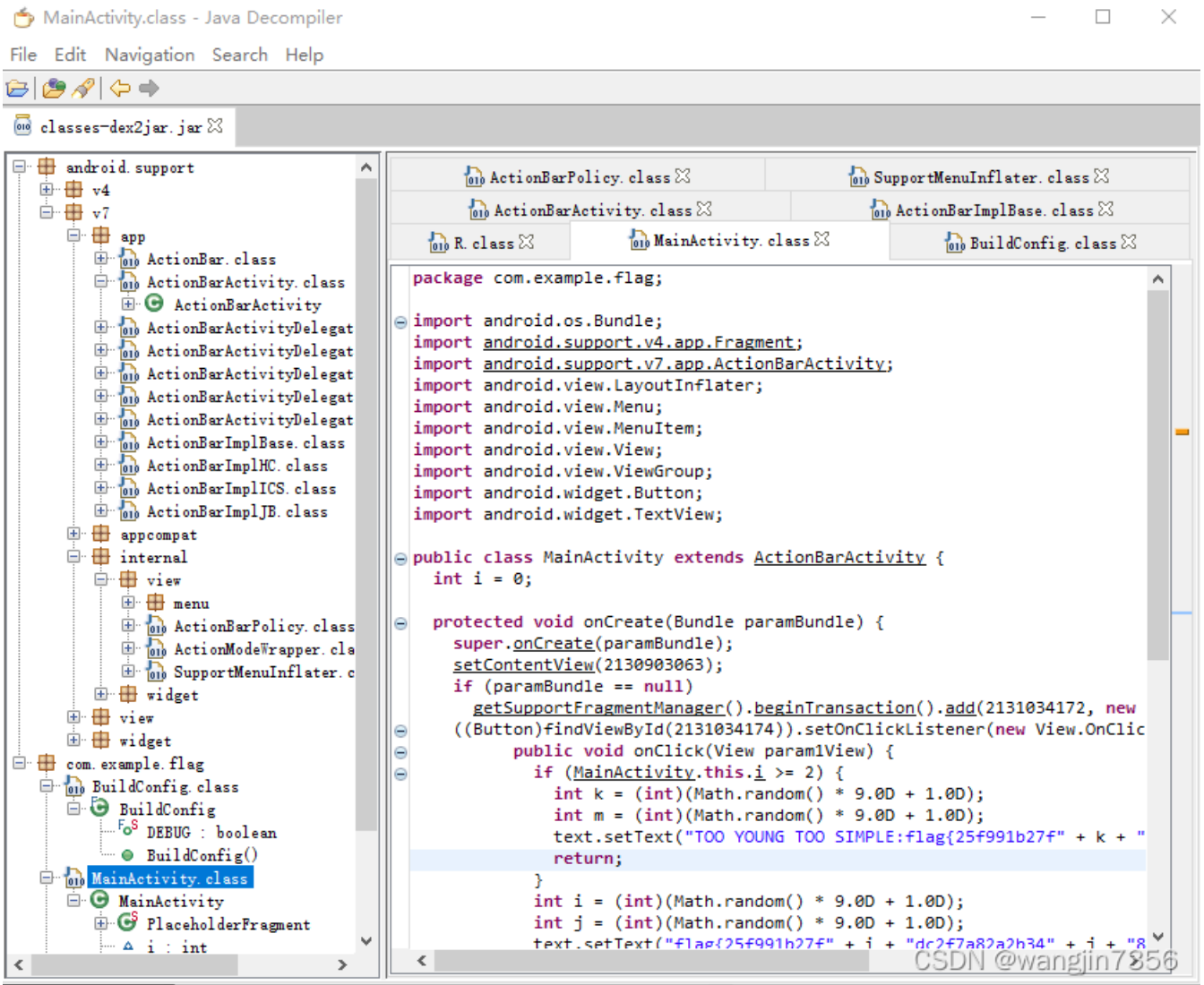
名称	修改日期	类型	大小
META-INF	2022/3/3 15:12	文件夹	
res	2022/3/3 15:12	文件夹	
1438.zip	2022/3/3 15:13	WinRAR ZIP 压缩...	680 KB
AndroidManifest.xml	2015/8/3 12:19	XML 文件	2 KB
classes.dex	2015/8/3 12:19	DEX 文件	1,241 KB
resources.arsc	2015/8/3 10:48	ARSC 文件	93 KB

CSDN @wangjin7356

应该是安卓逆向。第一步使用“dex2jar-2.0”工具，将classes.dex复制到dex2jar-2.0工具目录下，运行命令：

```
dex2jar-2.0\d2j-dex2jar.bat classes.dex
```

得到classes-dex2jar.jar文件。第二步使用“jd-gui”工具分析classes-dex2jar.jar文件



在MainActivity.class发现flag:

```

    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++;
        }
    });
}

```

CSDN @wangjin7356

根据题目提示，“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），应该就在k和m这两处”。最后得到flag:

flag{25f991b27fcdc2f7a82a2b34386e81c4}

小结

- 1.知识点：安卓逆向。“dex2jar-2.0”、“jd-gui”两个工具的使用。
- 2.解题过程并不复杂，最后暴力破解参考了别人的博客。