

攻防世界Misc入门题之坚持60s

原创

[沐一·林](#) 于 2021-08-11 21:24:26 发布 142 收藏

分类专栏: [CTF 杂项](#) 文章标签: [unctf](#)

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/xiao__1bai/article/details/119617278

版权



[CTF 同时被 2 个专栏收录](#)

167 篇文章 6 订阅

订阅专栏



[杂项](#)

19 篇文章 0 订阅

订阅专栏

攻防世界Misc入门题之坚持60s

继续开启全栈梦想之逆向之旅~

这题是攻防世界Misc入门题之坚持60s

坚持60s

👍 17

最佳Writeup由不要让我起名提供

WP

建议

难度系数: ★★★★★ 4.0

题目来源: 08067CTF

题目描述: 菜狗发现最近菜猫不爱理他, 反而迷上了菜鸡

题目场景: 暂无

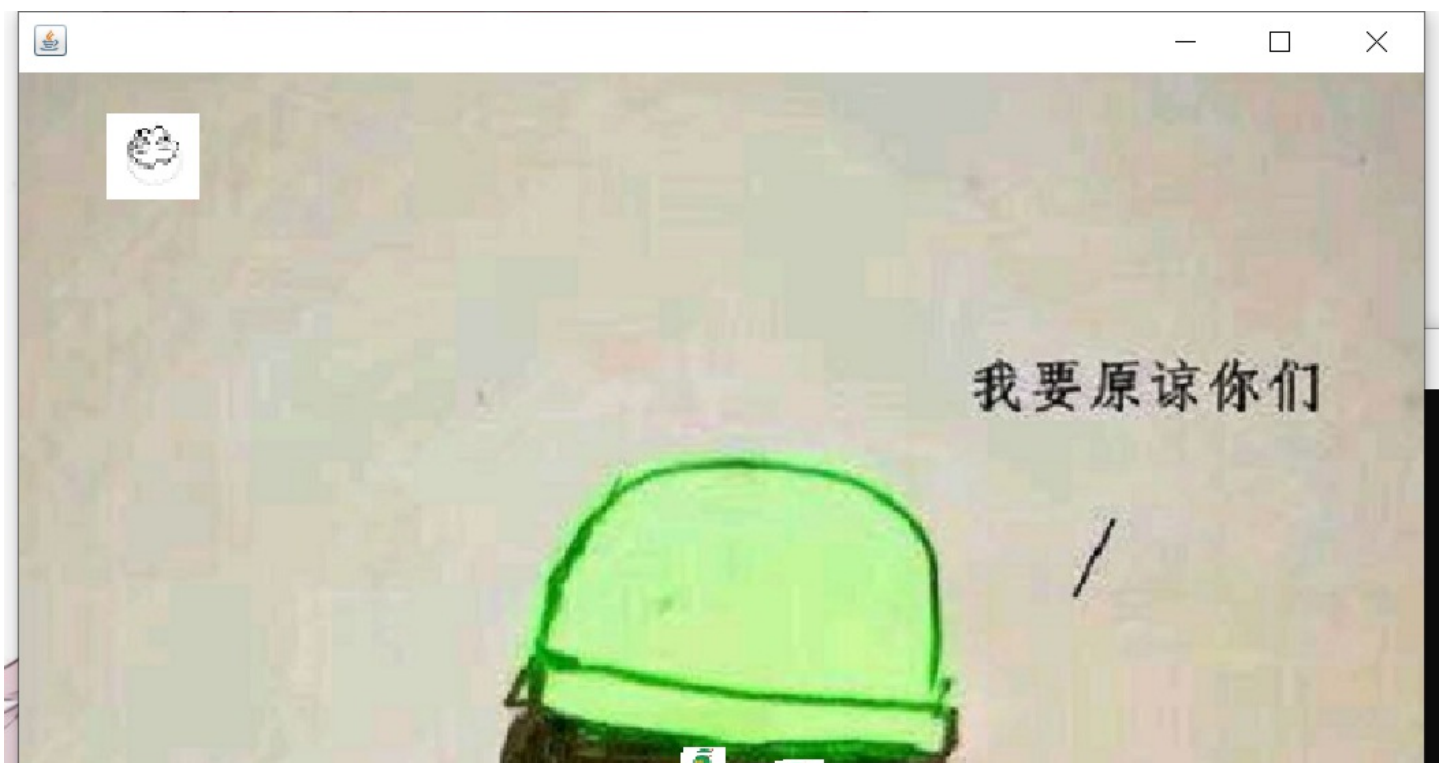
题目附件: 附件1

https://blog.csdn.net/xiao__1bai



下载附件, 一开始我默认用压缩包对jar文件, 搞到一解压出来还以为是某个游戏存档, 后来才发现是jar文件。
运行jar程序命令:

```
java -jar 文件名
```

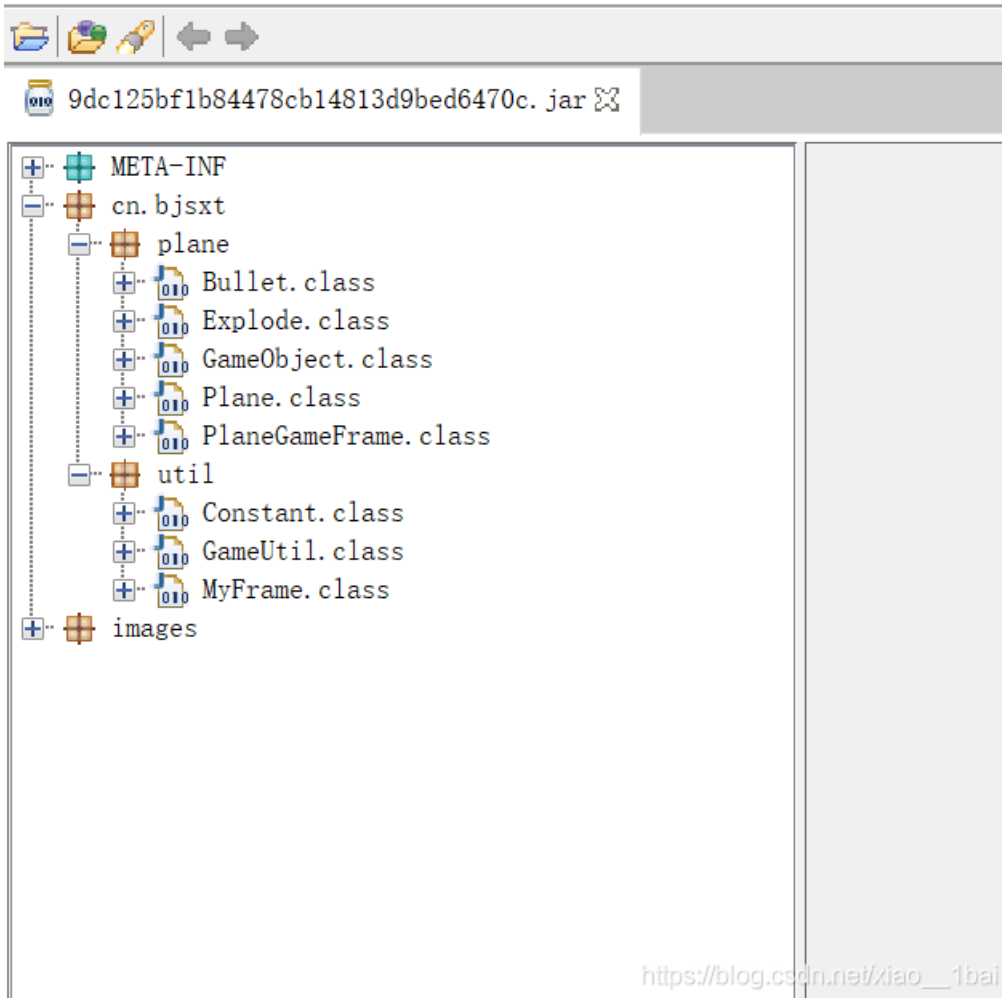




这种没用户输入的程序，flag通常要不是完整存在的字符串要不是根据时间推算出来的公式字符串。
所以查看源码，用jd-gui打开或直接拉到AndroidKiller中：

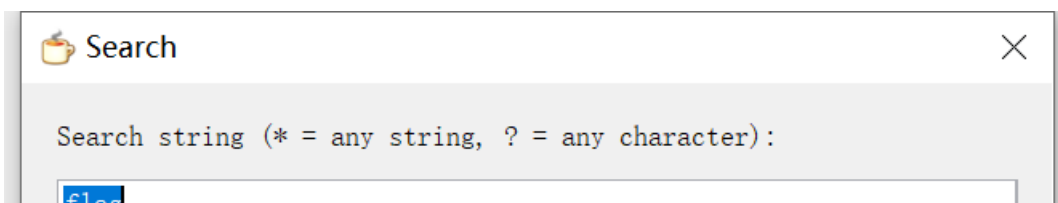
📁 9dc125bf1b84478cb14813d9bedb470c.jar - Java Decompiler

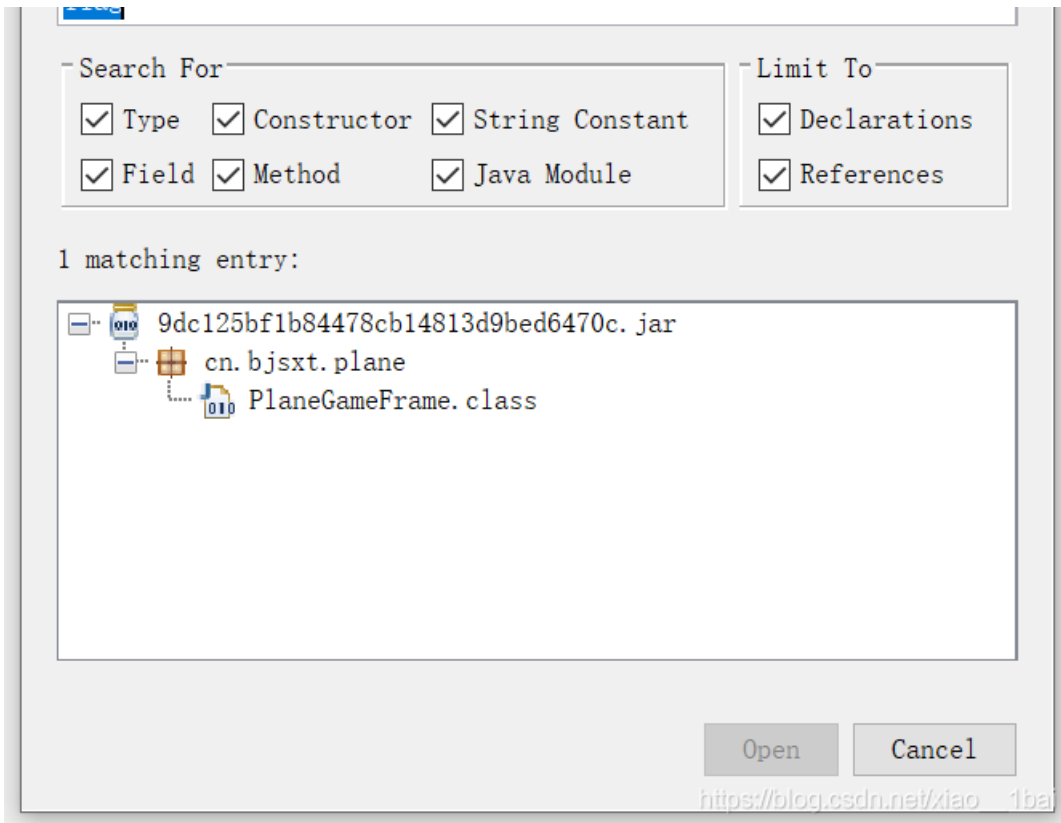
File Edit Navigation Search Help



猜测是完整存在的字符串，如果不是

再继续想：





搜索flag, 打开对应类:

```

    break;
    case 4:
        printInfo(g, "加油你就是下一个老王", 50, 150, 300);
        break;
    case 5:
        printInfo(g, "如果撑过一分钟我岂不是没面子", 40, 30, 300);
        break;
    case 6:
        printInfo(g, "Flag{RGFqURhbGlSmlud2FuQ2hpamk=}", 50, 150, 300);
        break;
    }
}
}

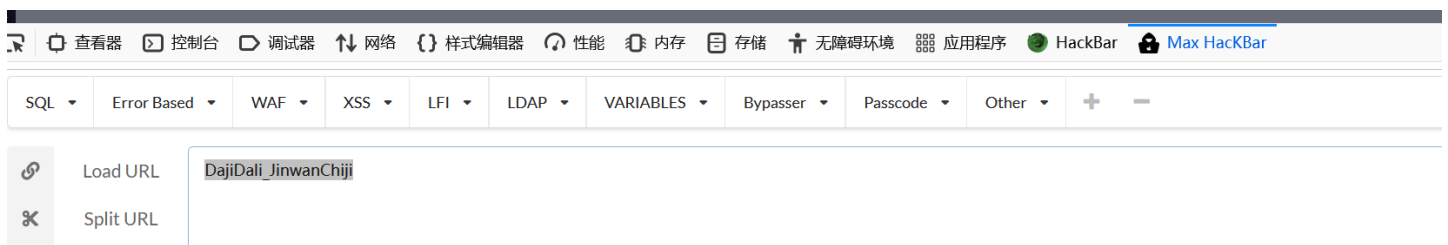
public void printInfo(Graphics g, String str, int size, int x, int y) {
90     Color c = g.getColor();
91     g.setColor(Color.RED);
92     Font f = new Font("宋体", 1, size);
93     g.setFont(f);
94     g.drawString(str, x, y);
95     g.setColor(c);
}

```

https://blog.csdn.net/xiao__1bai

有完整的flag, 因为题目说坚持60S, 所以这里也是在case 6处, 逻辑上符合。

直接提交, 直接报错, 人傻了, 看了wp才知道原来就算在flag中也还要base64解密, 我知道内容给你是base64, 但不知道是在flag{}的base64还要解密, 那就解嘛:



最后flag:

flag{DajiDali_JinwanChiji}



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)