




# 2021-02-18-ctf-坚持60s-反编译

原创

黑朱雀  于 2022-03-22 14:35:31 发布  3901  收藏 1

分类专栏: [网络安全](#) 文章标签: [ctf](#)

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/weixin\\_43639682/article/details/123660233](https://blog.csdn.net/weixin_43639682/article/details/123660233)

版权



[网络安全](#) 专栏收录该内容

25 篇文章 1 订阅

订阅专栏

layout: post

title: “ctf-坚持60s”

categories: [ctf]

tags: [反编译]

反编译:

反编译做的就是编译的相反动作。举例说, 例如一个程序用C语言写, 写完之后要编译成CPU可以识别和运行的机器代码, 也就是生成EXE程序。而反编译是反过来, 把EXE反编译成编程源代码, 也就是C程序, 不过一般反编译大多数都是从机器码反编译为汇编。其他语言的情况基本也是这样的。至于具体要怎么用, 这个就看你的目的了。但一般情况下是通过反编译主要是用于没有源码的程序的分析, 例如破解别人的软件等

Java 源代码编译后生成的 class 文件由于包含类名、方法名、变量等信息, 很容易被反编译, 且反编译后几乎可以达到与源代码一致的效果。对 Java 的 JAR 包、WAR 包进行保护。通过加密 Java 中每个方法的字节码防止反编译

[目标]

简单密码学

[环境]

windows

[工具]

jd-gui

Download Addr: <http://java-decompiler.github.io/>

[分析过程]

一个 java 小游戏, 用 jd-gui 打开, 直接搜索: flag, 得到, 结果需要 base64 解码。

a96f1888ba5349d9a3a54c07c47f244e.jar

- ⊕ META-INF
- ⊕ cn.bjstx
  - ⊕ plane
    - 📄 Bullet
      - 📄 Bullet
        - ▲ ball : Image
        - ▲ degree : double
        - ▲ height : int
        - ▲ img : Image
        - ▲ speed : int
        - ▲ width : int
        - ▲ x : double
        - ▲ y : double
        - Bullet()
        - draw(Graphics) : void
        - getRect() : Rectangle
      - 📄 Explode
      - 📄 GameObject
      - 📄 Plane
      - 📄 PlaneGameFrame
    - ⊕ util
    - ⊕ images

PlaneGameFrame.class

```

54     printInfo(g, "你的持久度才" + period + "秒", 50, 150, 250);
55     switch (period / 10)
56     {
57     case 0:
58         printInfo(g, "真.头顶一片青青草原", 50, 150, 300);
59         break;
60     case 1:
61         printInfo(g, "这东西你也要抢着带?", 50, 150, 300);
62         break;
63     case 2:
64         printInfo(g, "如果梦想有颜色, 那一定是原谅色", 40, 30, 300);
65         break;
66     case 3:
67         printInfo(g, "哟, 炊事班长呀兄弟", 50, 150, 300);
68         break;
69     case 4:
70         printInfo(g, "加油你就是下一个老王", 50, 150, 300);
71         break;
72     case 5:
73         printInfo(g, "如果撑过一分钟我岂不是很没面子", 40, 30, 300);
74         break;
75     case 6:
76         printInfo(g, "flag[RGFqaURhbGlfSmlud2FuQ2hpamk=]" 50, 150, 300);
77         break;
78     }
79     }
80 }
81
82 public void printInfo(Graphics g, String str, int size, int x, int y)
83 {
84     Color c = g.getColor();
85     g.setColor(Color.RED);
86     Font f = new Font("宋体", 1, size);
87     g.setFont(f);
88     g.drawString(str, x, y);
89     g.setColor(c);
90 }
91
92 }
93
94 }
95

```

DajiDali\_JinwanChiji

RGFqaURhbGlfSmlud2FuQ2hpamk=

多行



[创作打卡挑战赛](#) >  
[赢取流量/现金/CSDN周边激励大奖](#)