攻防世界 - MISC - 07 - 坚持60s

原创

古月浪子 于 2019-10-03 15:31:35 发布

分类专栏： 攻防世界CTF新手练习区 文章标签： 攻防世界 XCTF CTF WP writeup

本文链接：https://blog.csdn.net/tqydyqt/article/details/101996633

攻防世界 - MISC - 07 - 坚持60s

审题

思路

一看题目就知道应该是一个游戏，可以考虑使用某些手段通关获得flag，或者分析游戏文件找出flag

知识点

考查选手对jar文件的反编译能力

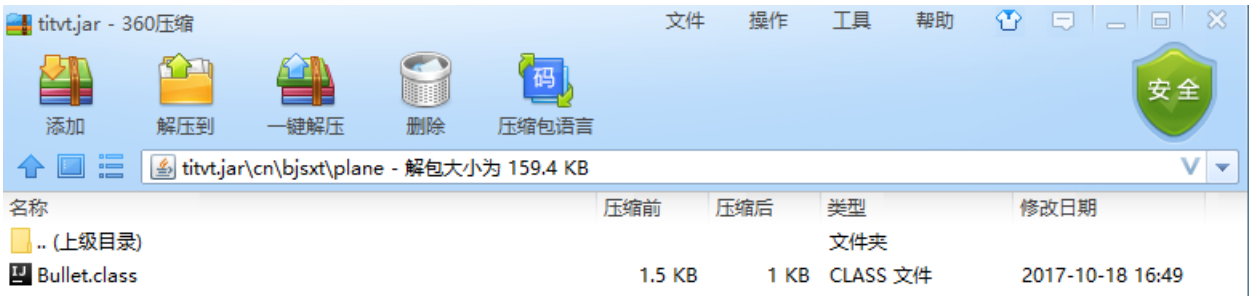
所需工具

IDEA

解题

直接运行附件，发现是个小游戏

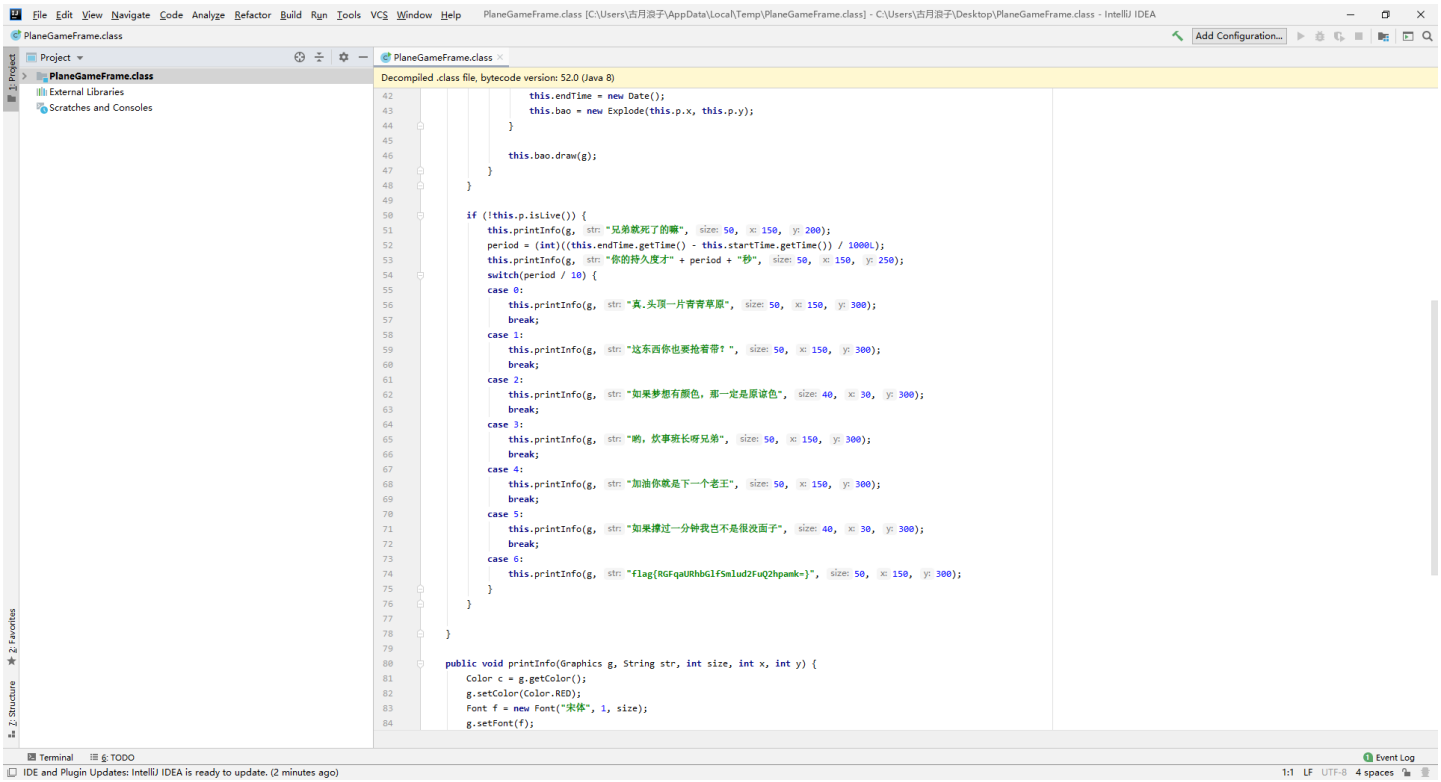
大致意思就是，你是左上角那个表情包，你要躲开那些绿帽并坚持60秒，通关就有flag
试了一下发现有点难。。。
用360压缩打开附件，找到PlaneGameFrame类并解压



Explode.class	1.3 KB	1 KB	CLASS 文件	2017-10-18 16:49
GameObject.class	1 KB	1 KB	CLASS 文件	2017-10-18 16:49
Plane.class	1.7 KB	1 KB	CLASS 文件	2017-10-18 16:49
PlaneGameFrame$KeyMonitor.class	1.6 KB	1 KB	CLASS 文件	2017-10-18 16:52
PlaneGameFrame.class	3.9 KB	2.3 KB	CLASS 文件	2017-10-18 16:52

大小: 124.0 KB 共 31 个文件和 6 个文件夹 压缩率 77.8% 已经选择 3.9 KB (1 个文件)

用IDEA打开class文件



```
                    this.endTime = new Date();
                    this.bao = new Explode(this.p.x, this.p.y);
                }

                this.bao.draw(g);
            }
        }

        if (!this.p.isLive()) {
            this.printInfo(g, str: "兄弟就死了的嘛", size: 50, x: 150, y: 200);
            period = (int)((this.endTime.getTime() - this.startTime.getTime()) / 1000L);
            this.printInfo(g, str: "你的持久度才" + period + "秒", size: 50, x: 150, y: 250);
            switch(period / 10) {
            case 0:
                this.printInfo(g, str: "真.头顶一片青青草原", size: 50, x: 150, y: 300);
                break;
            case 1:
                this.printInfo(g, str: "这东西你也要抢着带！", size: 50, x: 150, y: 300);
                break;
            case 2:
                this.printInfo(g, str: "如果梦想有颜色，那一定是原谅色", size: 40, x: 30, y: 300);
                break;
            case 3:
                this.printInfo(g, str: "哟，炊事班长呀兄弟", size: 50, x: 150, y: 300);
                break;
            case 4:
                this.printInfo(g, str: "加油你就是下一个老王", size: 50, x: 150, y: 300);
                break;
            case 5:
                this.printInfo(g, str: "如果撑过一分钟我岂不是很没面子", size: 40, x: 30, y: 300);
                break;
            case 6:
                this.printInfo(g, str: "flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}", size: 50, x: 150, y: 300);
            }
        }

    }

    public void printInfo(Graphics g, String str, int size, int x, int y) {
        Color c = g.getColor();
        g.setColor(Color.RED);
        Font f = new Font("宋体", 1, size);
        g.setFont(f);
```

老规矩，猜测这是一个base64编码，解码得到flag

flag

flag{DajiDali_JinwanChiji}

反思与心得

本来打算修改代码使绿帽不动的，后来发现flag就明文放在代码中，有些小题大做了,ε⊃ε,