bugku的做个游戏(08067CTF) writeup

原创

灵梦归希 于 2018-05-12 10:32:05 发布 4932 收藏 1
分类专栏： ctf writeup 文章标签： bugku writeup 08067CTF 做个游戏 heiheihei.jar

本文链接：https://blog.csdn.net/qq_30167299/article/details/80288904


ctf 同时被 2 个专栏收录
3 篇文章 0 订阅
订阅专栏


writeup
3 篇文章 0 订阅
订阅专栏

下载题目给的文件:heiheihei.jar

发现是java的jar文件，直接运行:

在控制台执行命令:java -jar heiheihei.jar

注:需要java运行环境,如果没有,先搭建java的环境。

题目说需要60s，额，有技术的话，玩60s应该是可以的，但本人没成功过60s。

然而，这游戏不知是bug还是彩蛋，可以躲在绿帽发现不了的地方，就是游戏的右边，一直往右边走，就会进入边界外面，绿帽过不去。

以为等一段时间，死了就有flag。没想到这是出题人的坑。

1.进去出不来

2.需要恰好60s.

还是另想办法：

使用binwalk分析下:binwalk heiheihei.jar

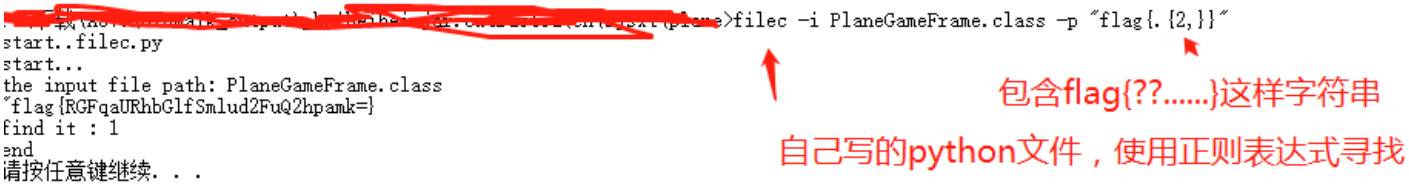
```
[redacted]>binwalk heiheihei.jar
* suggest: you'd better to input the parameters enclosed in double quotes.
* made by pcat
excute "[redacted]" heiheihei.jar

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, name: META-INF/MANIFEST.MF
148           0x94            Zip archive data, at least v1.0 to extract, name: cn/
181           0xB5            Zip archive data, at least v1.0 to extract, name: cn/bjsxt/
220           0xDC            Zip archive data, at least v1.0 to extract, name: cn/bjsxt/plane/
265           0x109           Zip archive data, at least v2.0 to extract, name: cn/bjsxt/plane/GameObject.class
850           0x352           Zip archive data, at least v2.0 to extract, name: cn/bjsxt/plane/Bullet.class
1856          0x740           Zip archive data, at least v2.0 to extract, name: cn/bjsxt/plane/Explode.class
2693          0xA85           Zip archive data, at least v2.0 to extract, name: cn/bjsxt/plane/PlaneGameFrame$KeyMonitor
3628          0xE2C           Zip archive data, at least v2.0 to extract, name: cn/bjsxt/plane/PlaneGameFrame.class
6044          0x179C          Zip archive data, at least v2.0 to extract, name: cn/bjsxt/plane/Plane.class
7091          0x1BB3          Zip archive data, at least v1.0 to extract, name: cn/bjsxt/util/
7135          0x1BDF          Zip archive data, at least v2.0 to extract, name: cn/bjsxt/util/Constant.class
7473          0x1D31          Zip archive data, at least v2.0 to extract, name: cn/bjsxt/util/GameUtil.class
8117          0x1FB5          Zip archive data, at least v2.0 to extract, name: cn/bjsxt/util/MyFrame$1.class
8606          0x219E          Zip archive data, at least v2.0 to extract, name: cn/bjsxt/util/MyFrame$PaintThread.class
9163          0x23CB          Zip archive data, at least v2.0 to extract, name: cn/bjsxt/util/MyFrame.class
9966          0x26EE          Zip archive data, at least v1.0 to extract, name: images/
10003         0x2713          Zip archive data, at least v2.0 to extract, name: images/ball.png
11817         0x2E29          Zip archive data, at least v2.0 to extract, name: images/bg.jpg
110295        0x1AED7         Zip archive data, at least v2.0 to extract, name: images/plane.png
112938        0x1B92A         Zip archive data, at least v1.0 to extract, name: images/explode/
112983        0x1B957         Zip archive data, at least v2.0 to extract, name: images/explode/e1.gif
113354        0x1BACA         Zip archive data, at least v2.0 to extract, name: images/explode/e10.gif
113411        0x1BB03         GIF image data, version "89a", 71 x 100
114752        0x1C040         Zip archive data, at least v2.0 to extract, name: images/explode/e11.gif
114809        0x1C079         GIF image data, version "89a", 71 x 100
116061        0x1C55D         Zip archive data, at least v2.0 to extract, name: images/explode/e12.gif
116118        0x1C596         GIF image data, version "89a", 71 x 100
117276        0x1CA1C         Zip archive data, at least v2.0 to extract, name: images/explode/e13.gif
117333        0x1CA55         GIF image data, version "89a", 71 x 100
118371        0x1CE63         Zip archive data, at least v2.0 to extract, name: images/explode/e14.gif
```

好多东西，直接使用命令:binwalk -e heiheihei.jar

分离出文件，其中一个文件\cn\bjsxt\plane下的PlaneGameFrame.class(为啥是这文件，一个一个试的)

寻找字符串,这里寻找的包含flag{***},***至少为2个字符的字符串。

可以使用你们自己的16进制编辑器，搜索flag也行。



得到flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}

RGFqaURhbGlfSmlud2FuQ2hpamk=进行base64编码

解码如下:DajiDali_JinwanChiji

flag提交就行：flag{DajiDali_JinwanChiji}