# jarvis oj reverse Fibonacci writeup

原创

charlie_heng 于 2018-02-22 09:45:12 发布 269 收藏

分类专栏： 二进制-逆向工程



本文链接：https://blog.csdn.net/charlie_heng/article/details/79345570



二进制-逆向工程 专栏收录该内容

34 篇文章 3 订阅

订阅专栏

这题之前也做过，不过卡了一下，现在再做，发现又会做了

首先要先把加密的class从exe里面dump出来

这里有个教程

http://reverseengineeringtips.blogspot.co.uk/2014/12/unpacking-jar2exe-21-extracting-jar.html

因为这个版本是x64的，所以断点停的是dec r8d


停住之后，在内存那里查看rsi的东西，rax就是原来jar的大小，直接dump下来

然后用7zip解压出几个文件，其中两个文件就是class，只要把后缀改成class ，用jd-gui 查看，然后复制代码到eclipse那里，运行一下就能出flag了