

BUUCTF-Reverse easyre1

原创

柒熠染云 于 2021-05-19 20:21:36 发布 123 收藏

分类专栏: [逆向工程](#) 文章标签: [安全 c语言](#)

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/m0_46276093/article/details/117044977

版权



[逆向工程](#) 专栏收录该内容

10 篇文章 1 订阅

订阅专栏

BUUCTF-Reverse easyre1

所用软件

1.IDA PRO (静态分析工具)

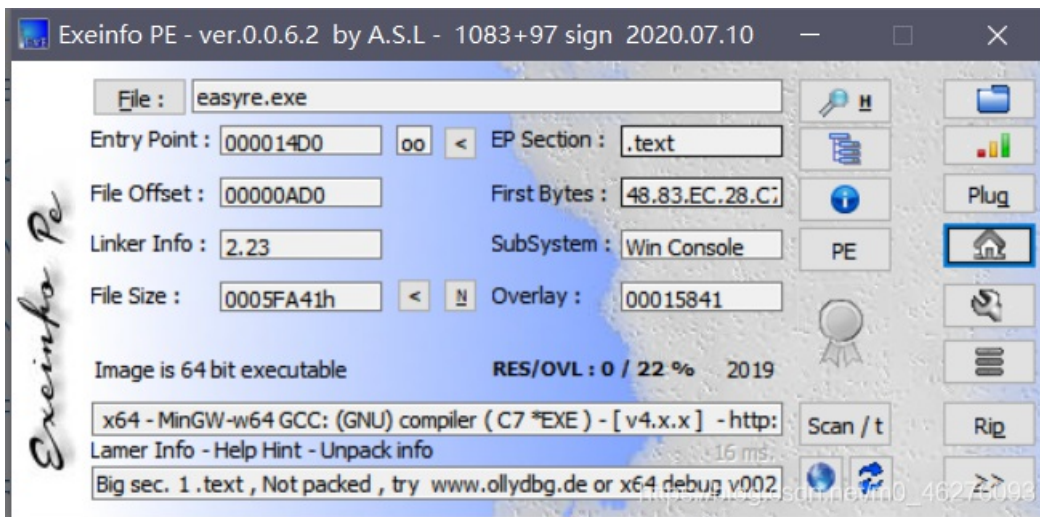
2.exeinfope (查壳工具)

操作步骤

1.下载easyre.exe并将其打开

(只有控制台, 无提示信息)

2.将easyre.exe放入exeinfope中查壳



发现程序没有加壳, 直接放入IDA中进行静态分析。

3.静态分析

进入IDA中后, 摁Shift+F12, 查看程序所包含字符串。

Address	Length	Type	String
.rdata:000000...	00000017	C	flag{this_is_a_EaSyRe}
.rdata:000000...	00000019	C	sorry,you can't get flag
.rdata:000000...	0000000F	C	std::exception
.rdata:000000...	00000013	C	std::bad_exception
.rdata:000000...	0000000B	C	eh_globals
.rdata:000000...	00000024	C	__gnu_cxx::__concurrency_lock_error
.rdata:000000...	00000026	C	__gnu_cxx::__concurrency_unlock_error
.rdata:000000...	0000001C	C	pure virtual method called

找到flag{this_is_a_EaSyRe}