

bugku-writeup-Reverse-Easy_Re

原创

dark2019 于 2021-06-27 16:04:56 发布 39 收藏

分类专栏: [信息安全 wp](#) 文章标签: [wp](#)

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/qq_22597955/article/details/118274067

版权



[信息安全](#) 同时被 2 个专栏收录

53 篇文章 1 订阅

订阅专栏



[wp](#)

31 篇文章 0 订阅

订阅专栏

题目: Easy_Re

Easy_Re

Reverse

已解决

分数: 15

金币: 2

题目作者: 未知

一血: [blacksugar](#)

一血奖励: 2金币

解决: 942

提示:

描述: flag格式: DUTCTF{xxxx}

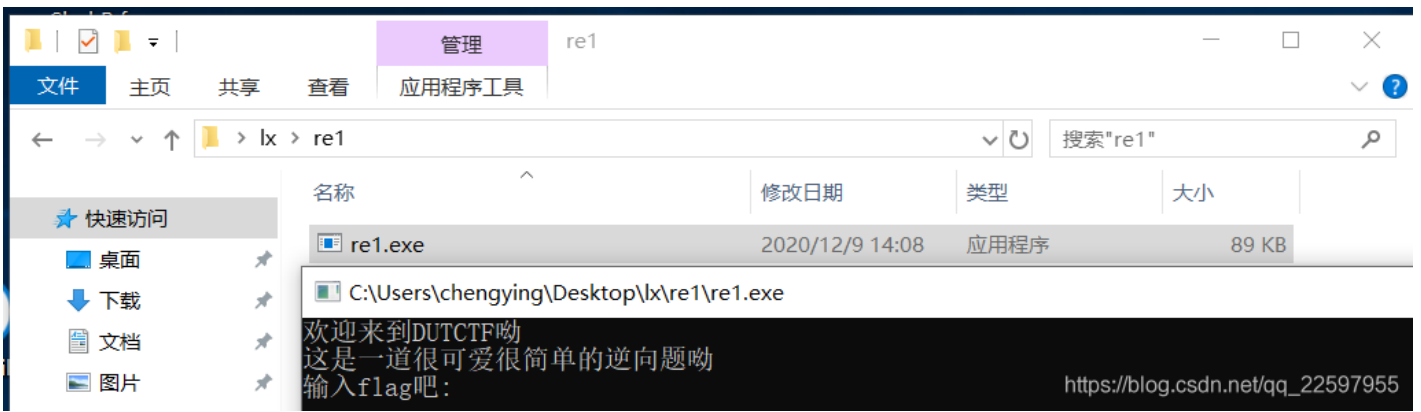
其他: [↓ 下载](#)

请输入flag

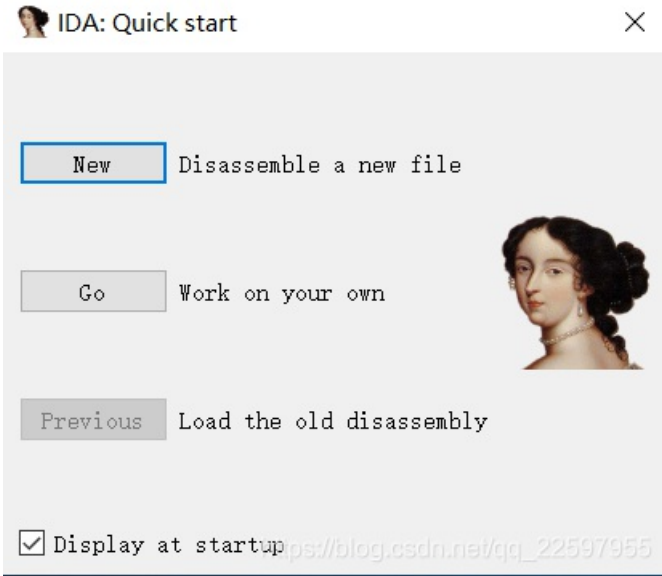
提交

https://blog.csdn.net/qq_22597955

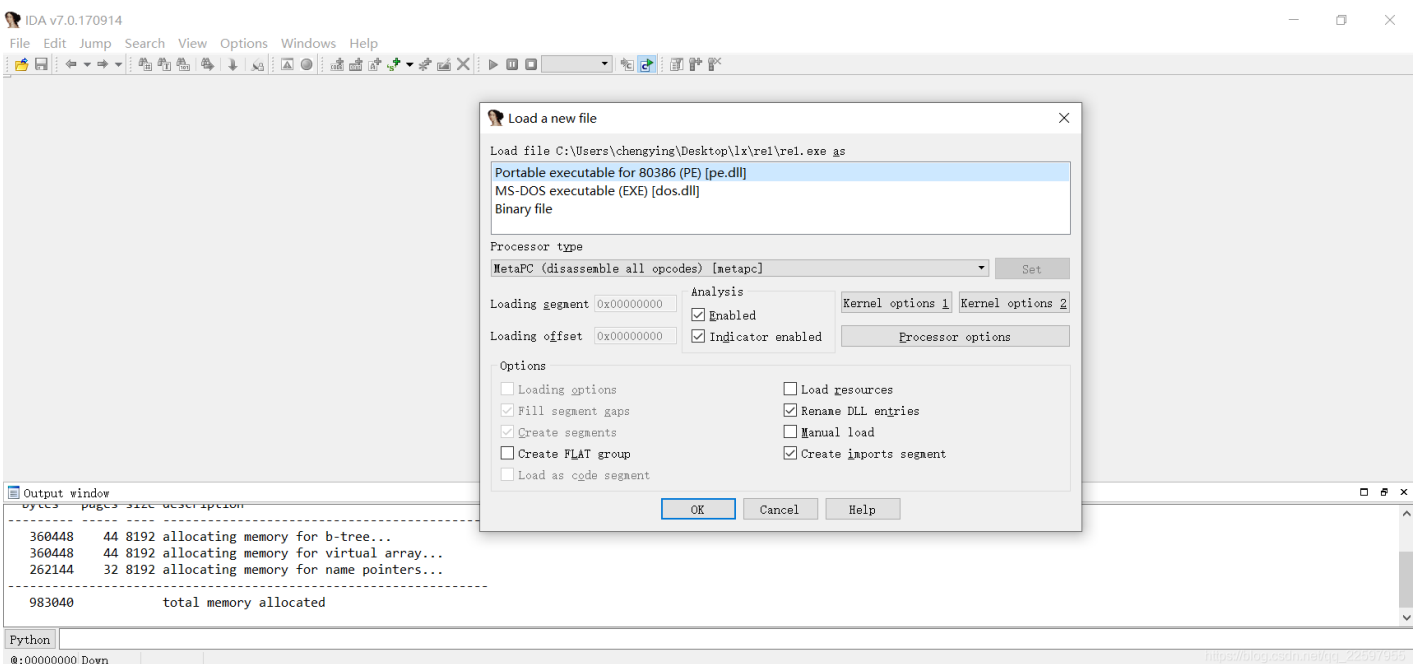
01—逆向解析



a. 下载题目中的压缩包，解压得到re1.exe, 双击运行查看得到如上信息。



b. 双击运行IDA Pro(32-bit), 打开新文件。



c. 直接点击ok

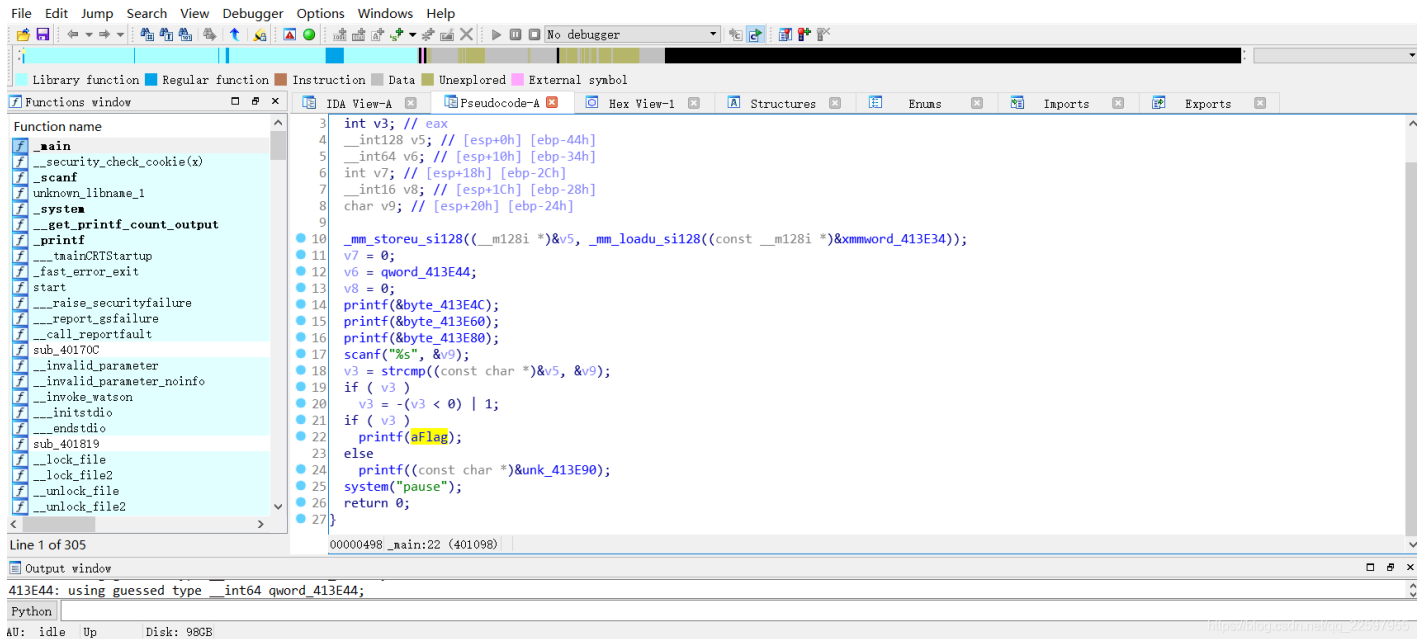
Please confirm



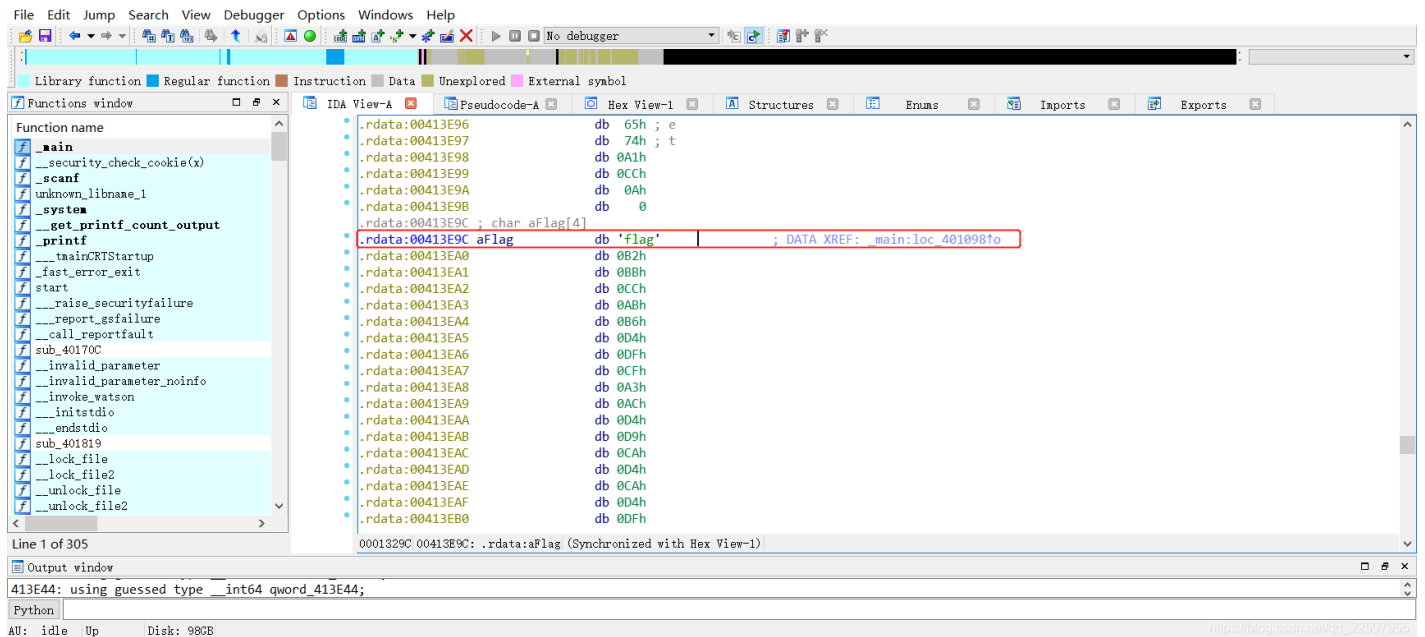
The input file was linked with debug information and the symbol filename is: 'E:\c\ConsoleApplication2\Release\ConsoleApplication2.pdb' Do you want to look for this file at the specified path and the Microsoft Symbol Server?

Don't display this message again

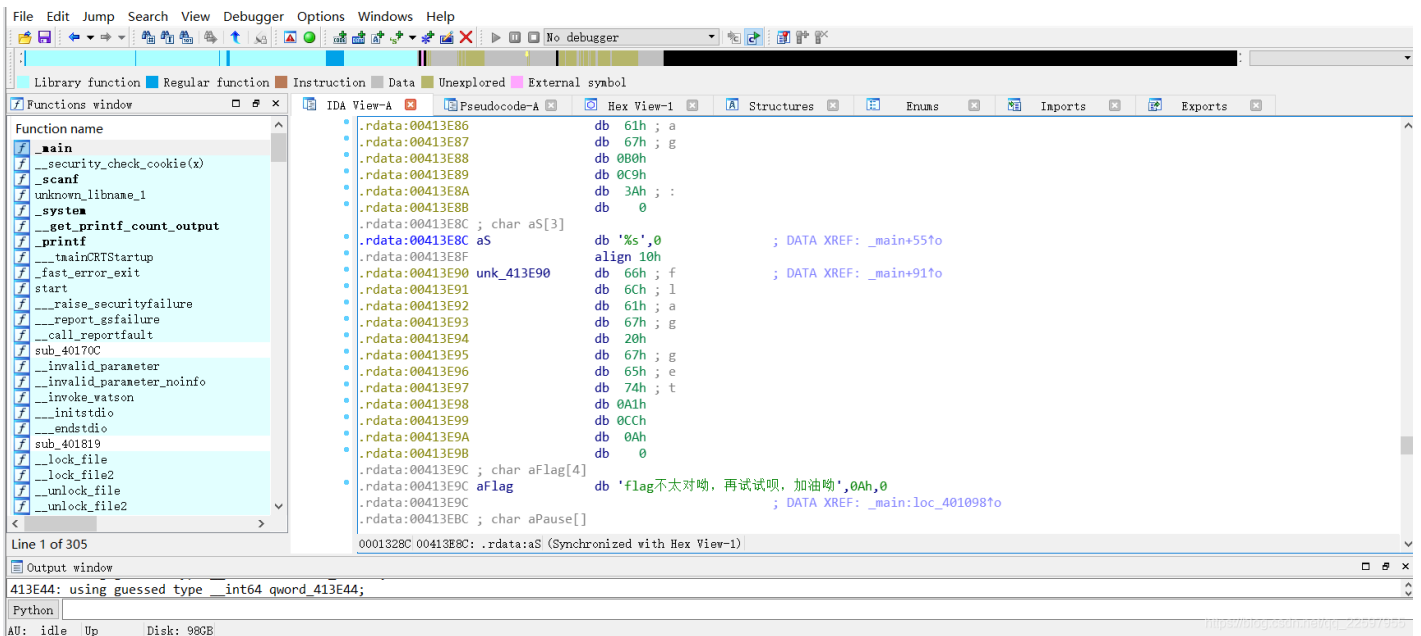
d.选yes



e.按F5打开伪代码，发现aFlag

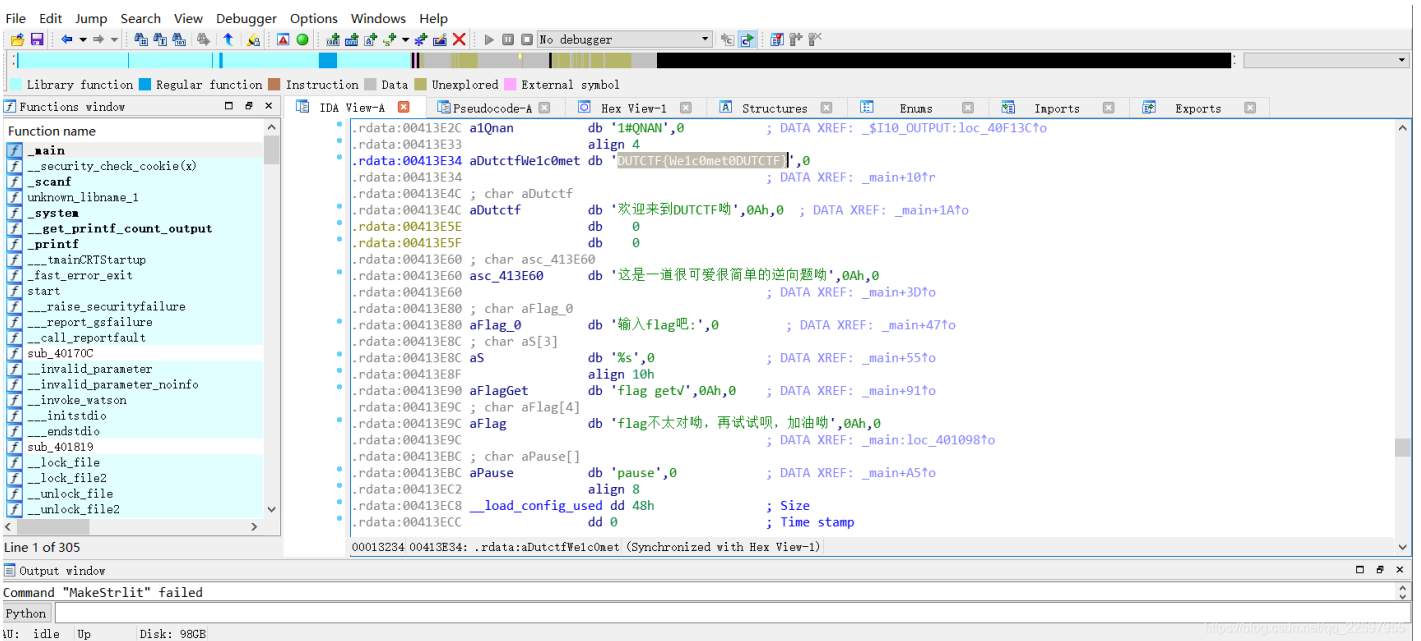


f.双击aFlag进入IDA View-A



g.按A键转为字符串，显示：flag不太对哟，再试试呗，加油哟

说明flag在前面。



02—逆向工具使用

IDA的一些快捷键：

找主函数：f5

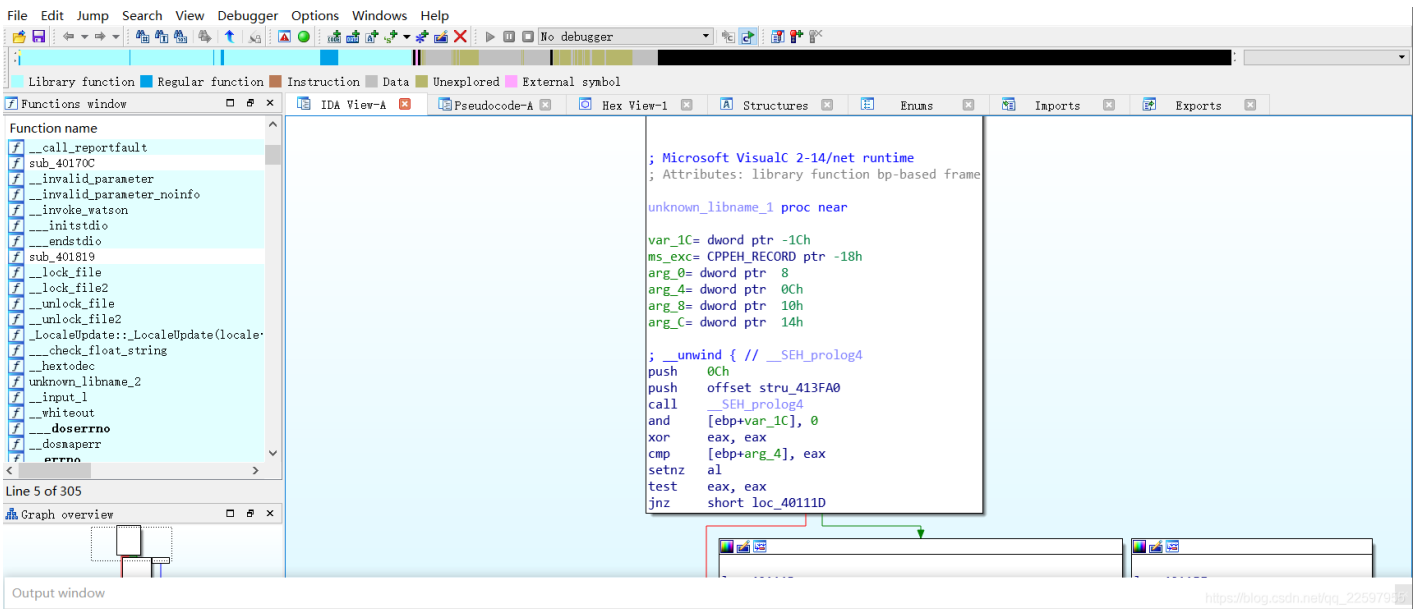
查找字符串：alt + t

转换字符串：A

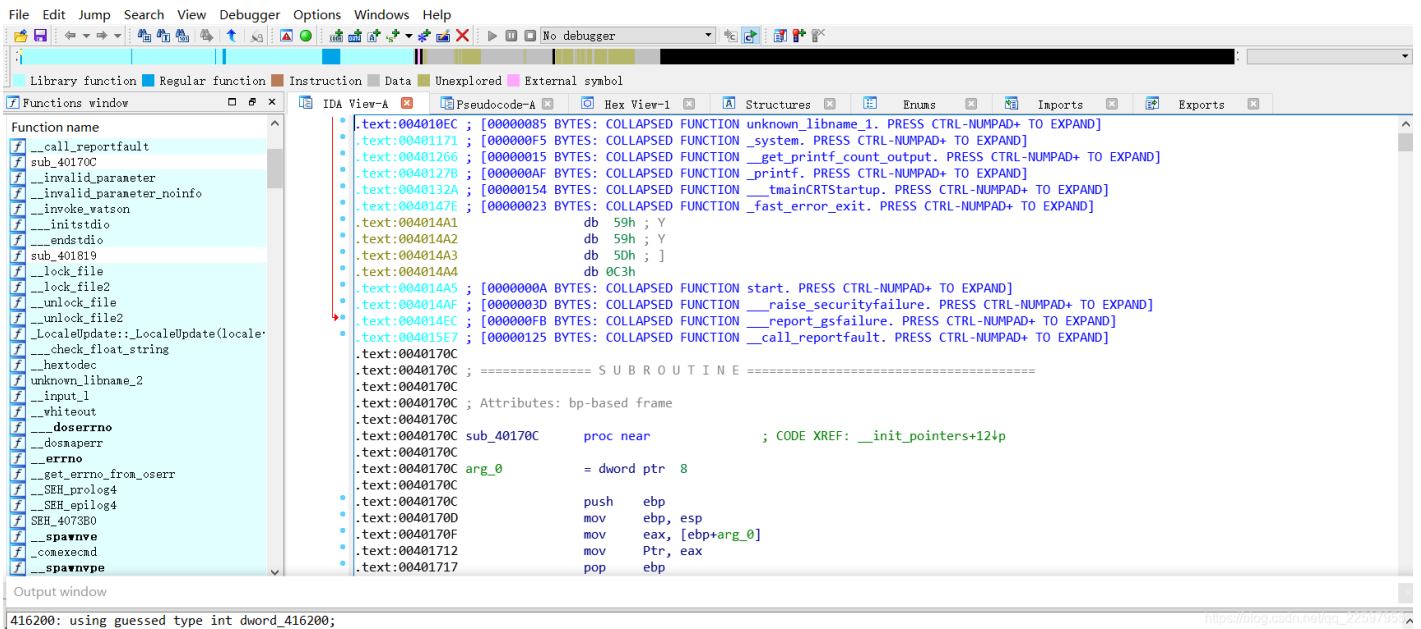
空格键:切换文本视图与图表视图

对变量进行字符转换:r

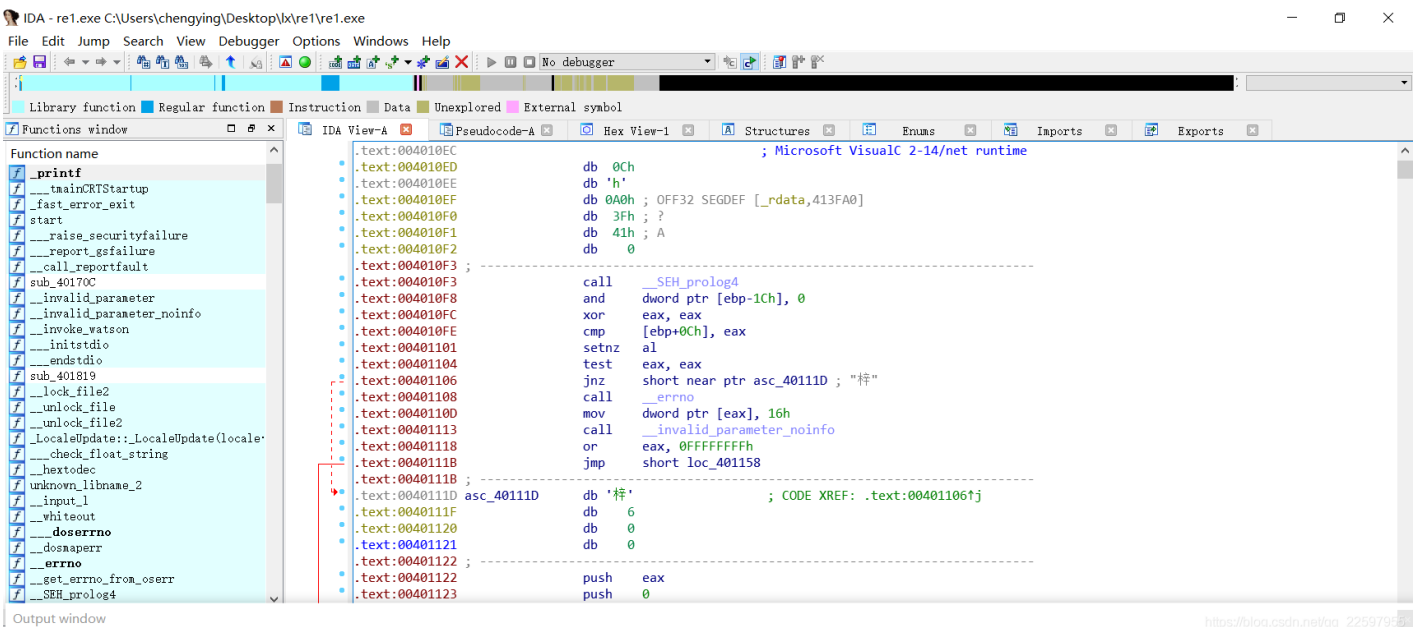
示例：



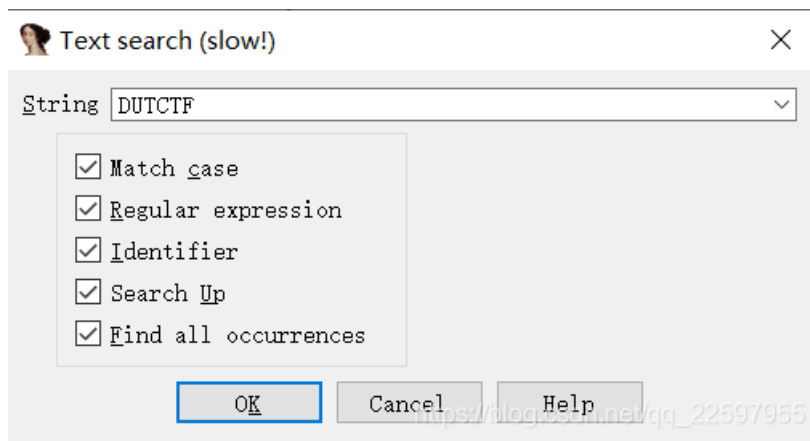
查看IDA View-A,处于图标视图界面,不便于查看,转为文本视图。



按空格键转为文档界面。



按A键转换为字符串。



按alt+t,查找文本。

ps:由于刚开始做逆向题，解析写的比较详细，工具的部分持续补充。