BUUCTF justRE

原创

一夜通宵程序员 于 2021-05-11 16:45:41 发布 134 收藏

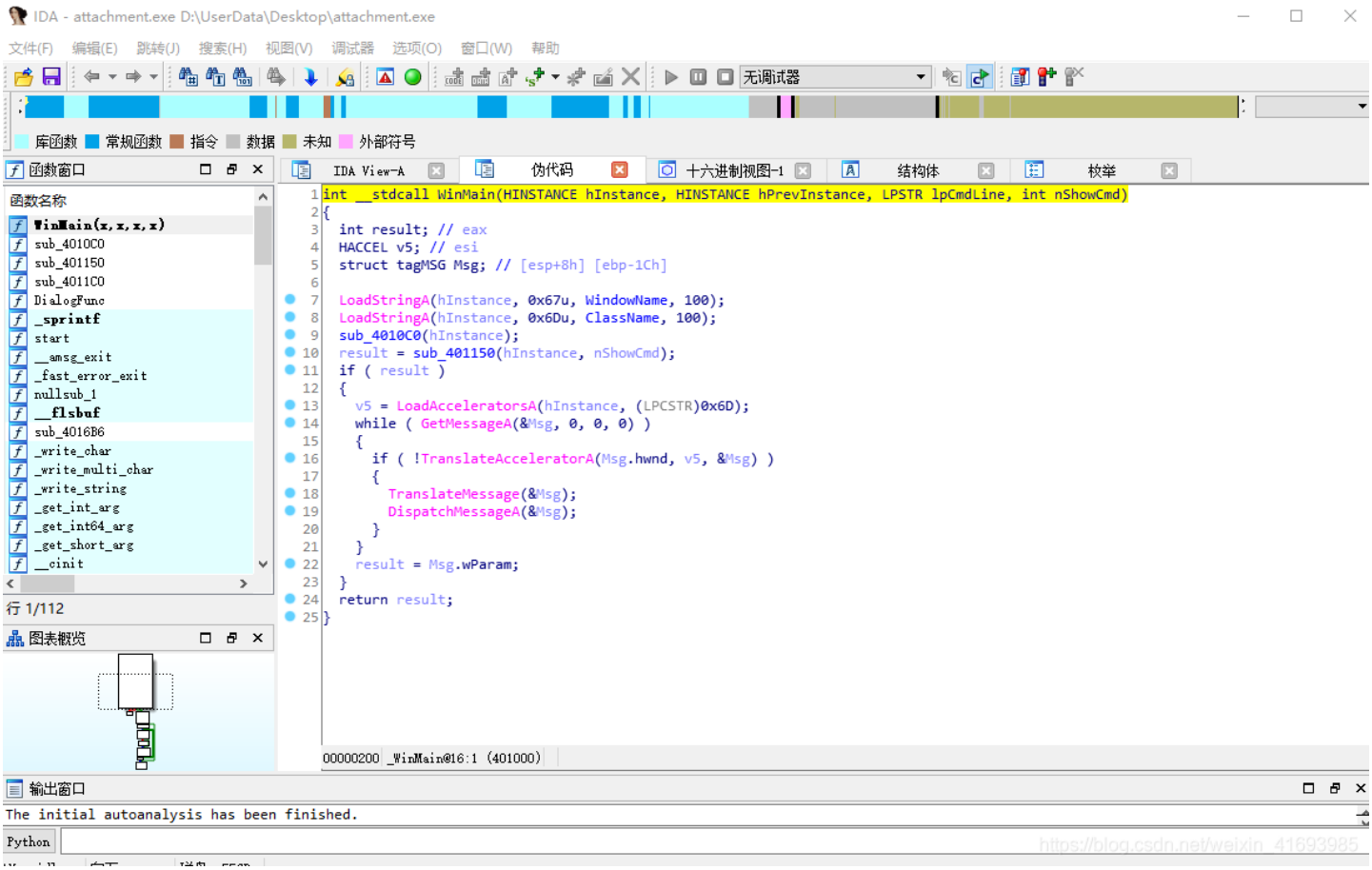
文章标签： c++

本文链接：https://blog.csdn.net/weixin_41693985/article/details/116660444

BUUCTF justRE

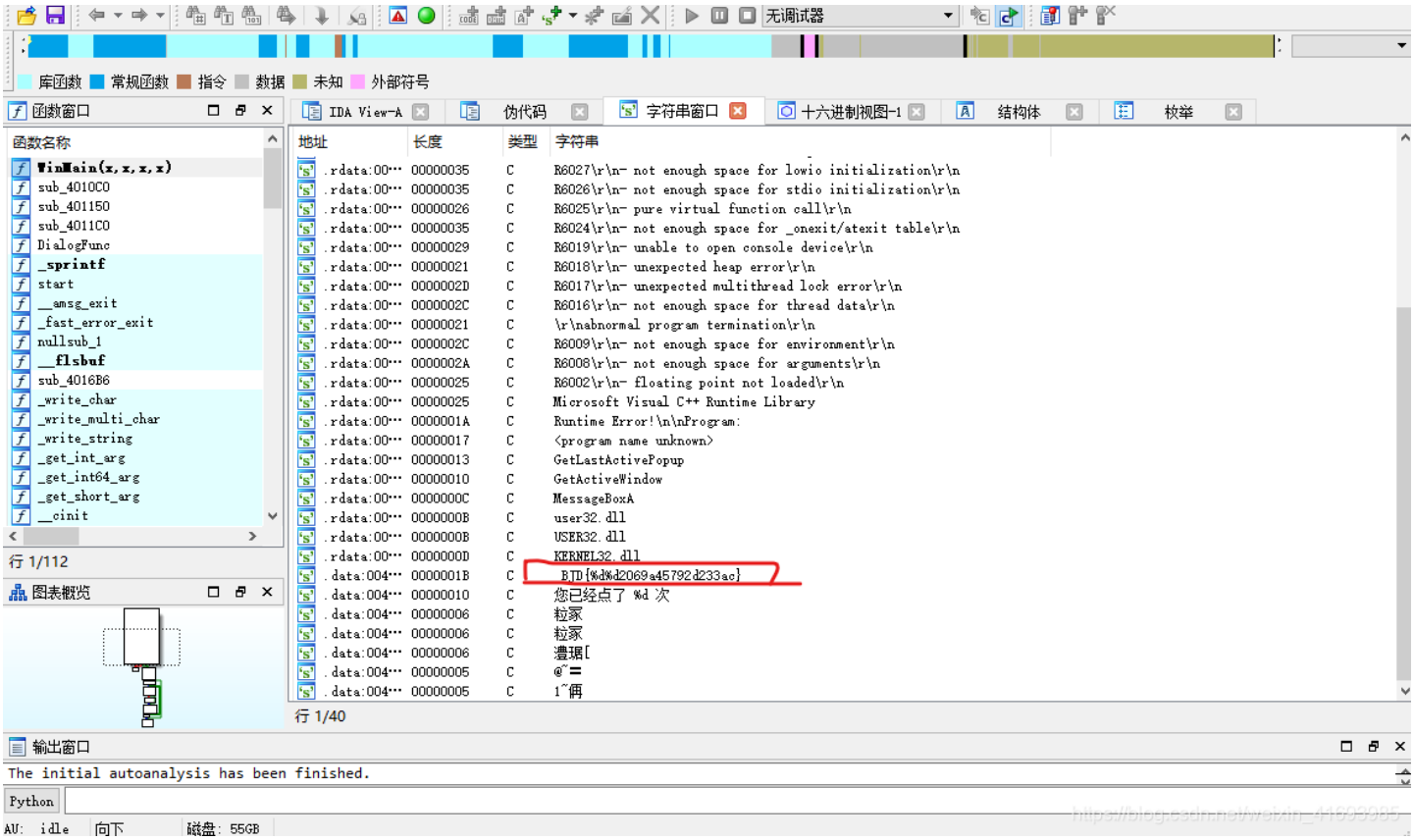
拿到程序照例查壳，无壳，32位程序

拖入ida



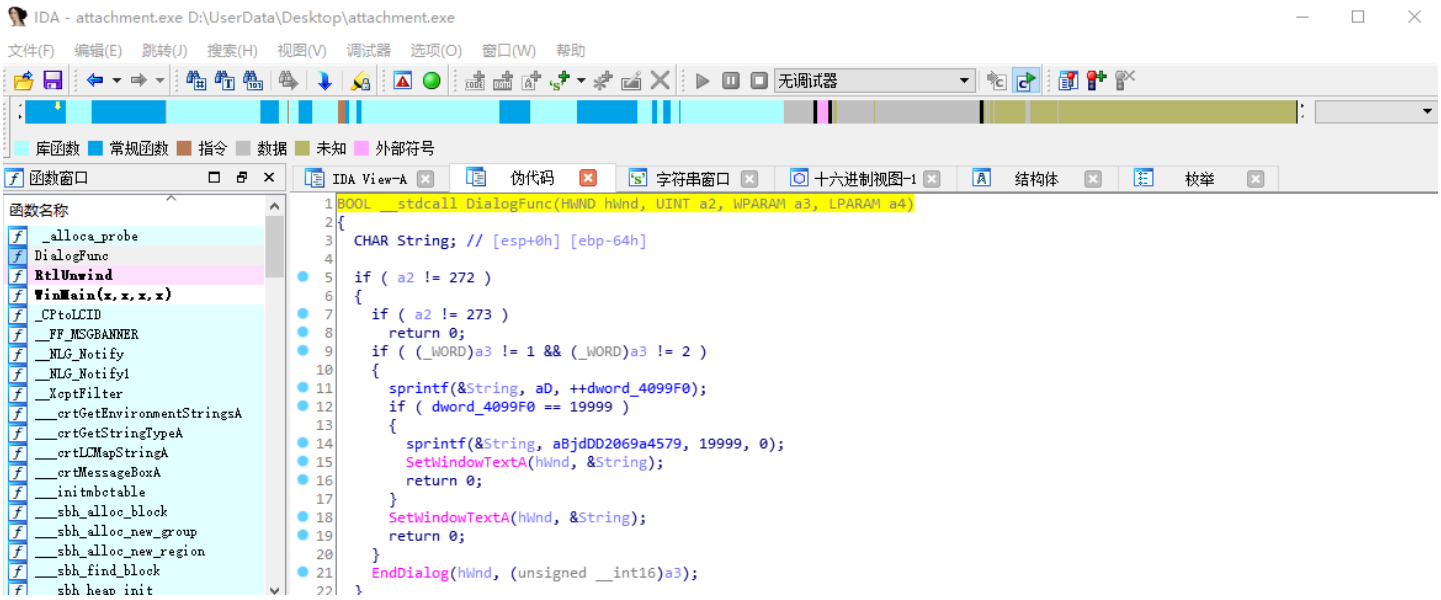
看了半天没看出什么有用的信息

CTRL+f12查找字符串，看到一串类似flag的字符串：BJD{%d%d2069a45792d233ac}

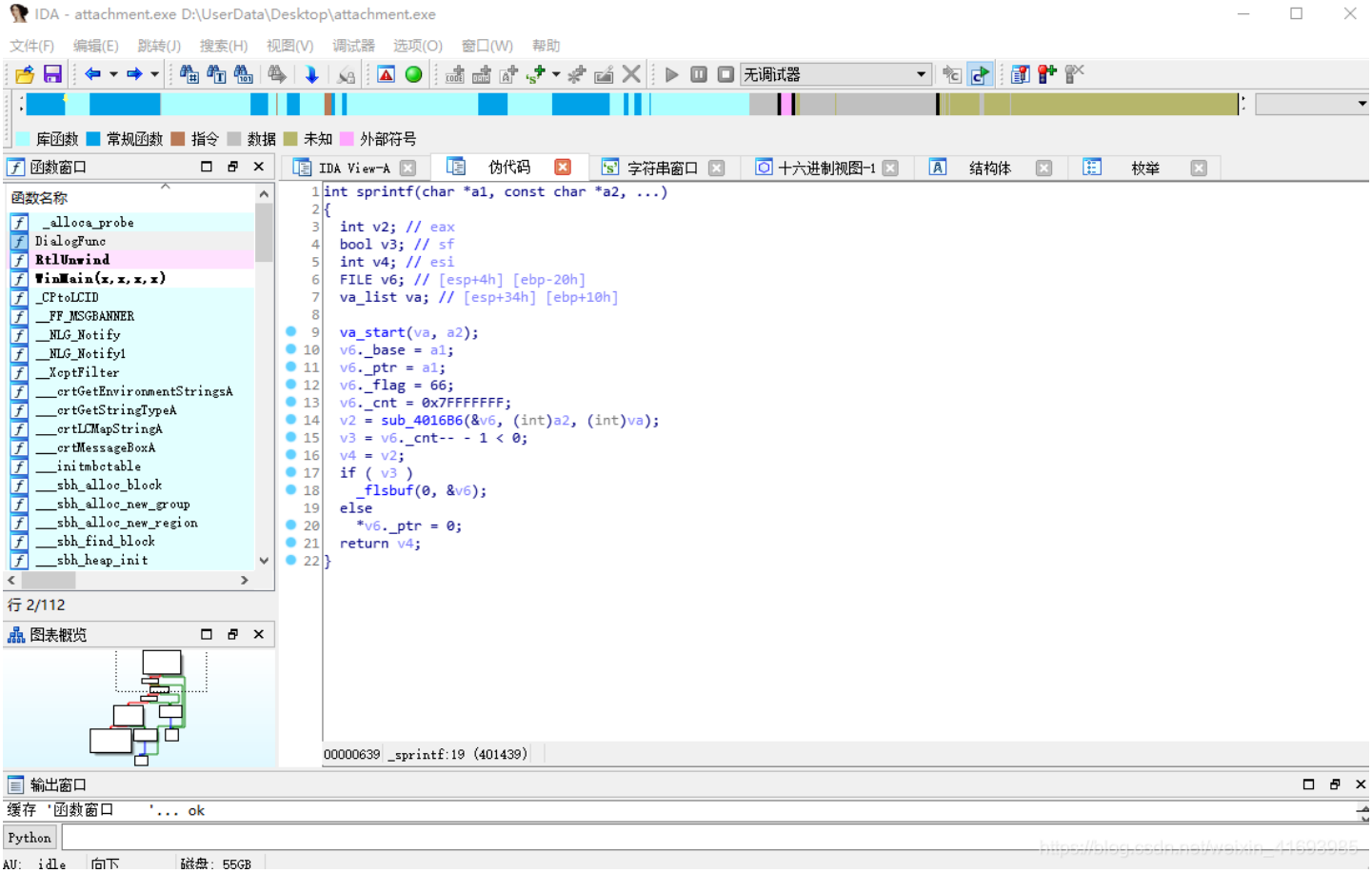


双击跟进，看到这串字符串的调用函数

跟进函数体

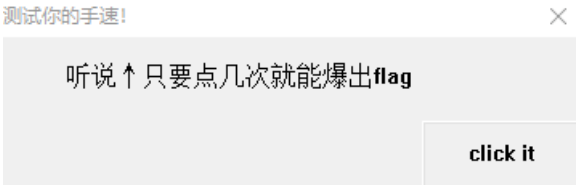


跟进sprintf函数



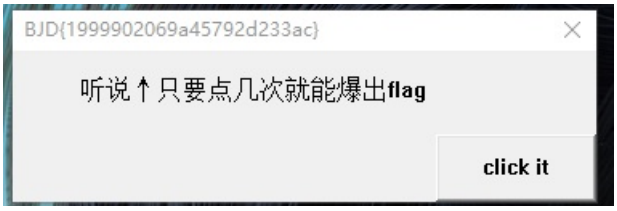
没看懂什么意思，转换思路，打开调试程序

看到getflag，点击跟进



点击可以出flag，好吧，软的不行那就只能硬来了

之前反汇编时在sprintf里面的参数中传入了19999，0这两个整数参数，大胆猜测点击19999次就可以出flag，编程制作连点器，点了19999次后



ok，flag出来了

总结：正向不行，逆向真的会瘸