

# XCTF-Reverse-ExerciseArea-003-writeup

原创

y4ung  于 2019-07-29 09:33:24 发布  4240  收藏

分类专栏: [ctf](#) 文章标签: [CTF ReverseEngineering](#)

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\\_35056292/article/details/97623365](https://blog.csdn.net/qq_35056292/article/details/97623365)

版权



[ctf](#) 专栏收录该内容

35 篇文章 0 订阅

订阅专栏

## 0x00 介绍

本题是xctf攻防世界中Reverse的新手第三题。

对给定的helloctf.exe进行逆向分析, 找到serial。

实验环境: IDA Pro 7.0

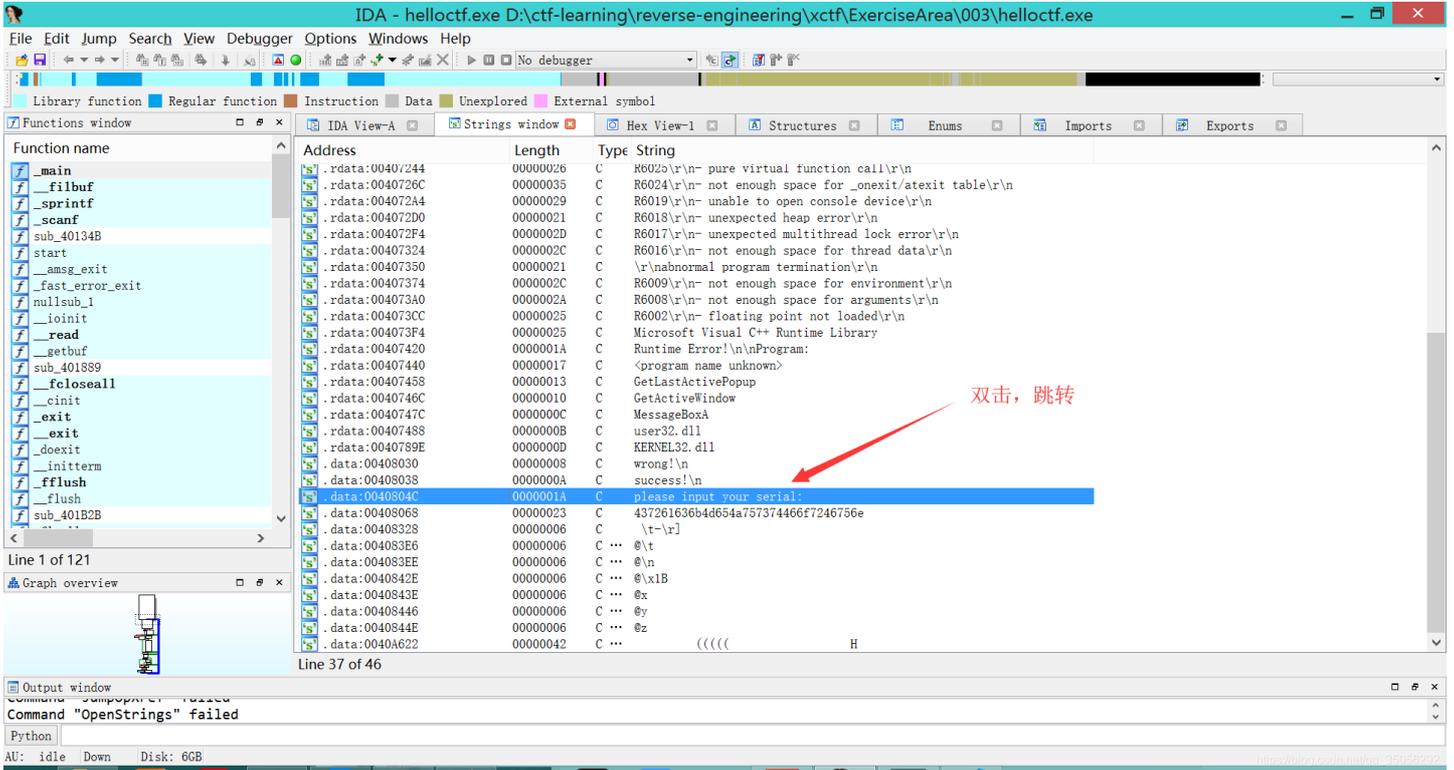
## 0x01 解题过程

### 1.1 前期的分析

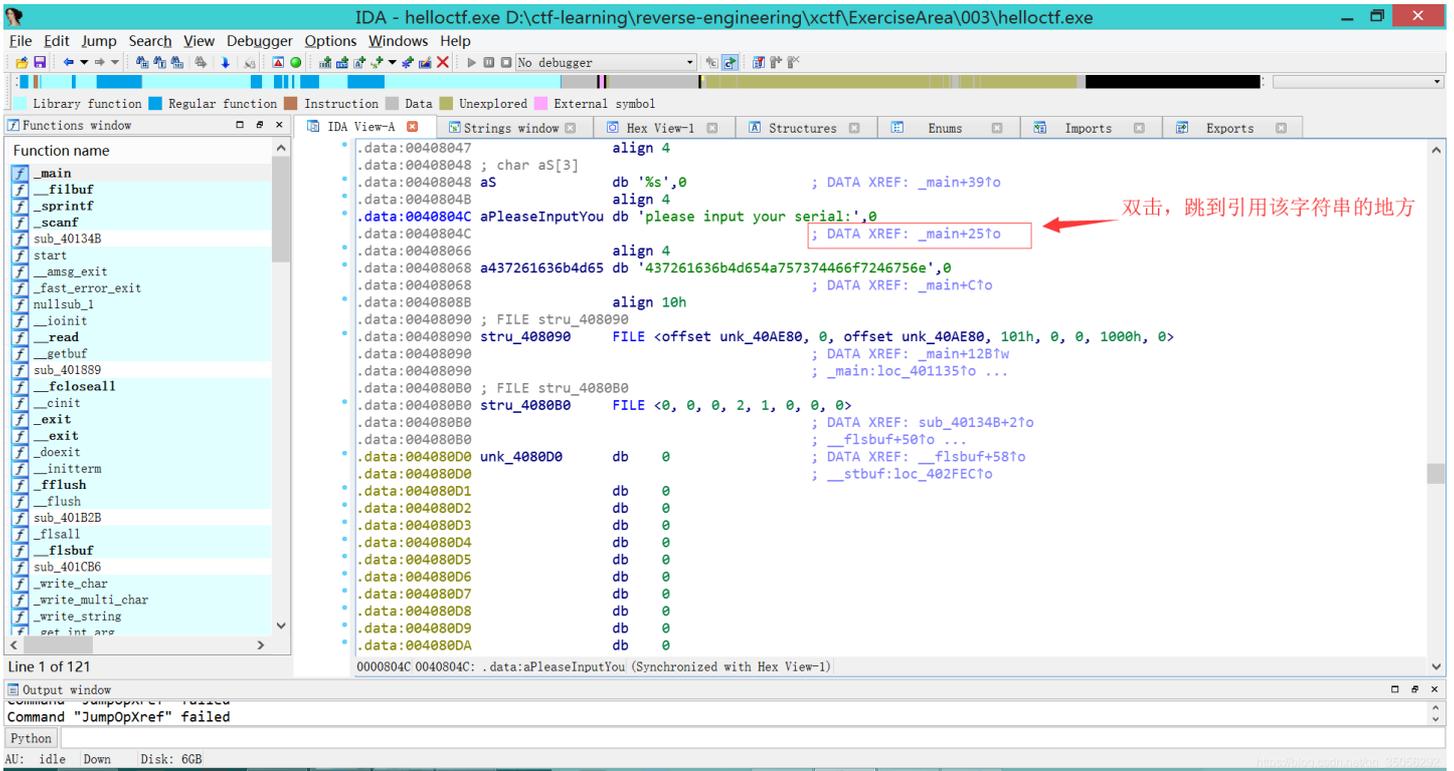
运行helloctf.exe, 可以看到需要输入serial, 如果输错的话会进入下一次循环判断

```
cmd - helloctf.exe
<1> cmd - helloctf...
振洋@LENOVO-HZY D:\ctf-learning\reverse-engineering\xctf\ExerciseArea\003
$ helloctf.exe
please input your serial:abcdefg
wrong!
please input your serial:abc
wrong!
please input your serial:
helloctf.exe*[32]:7336
```

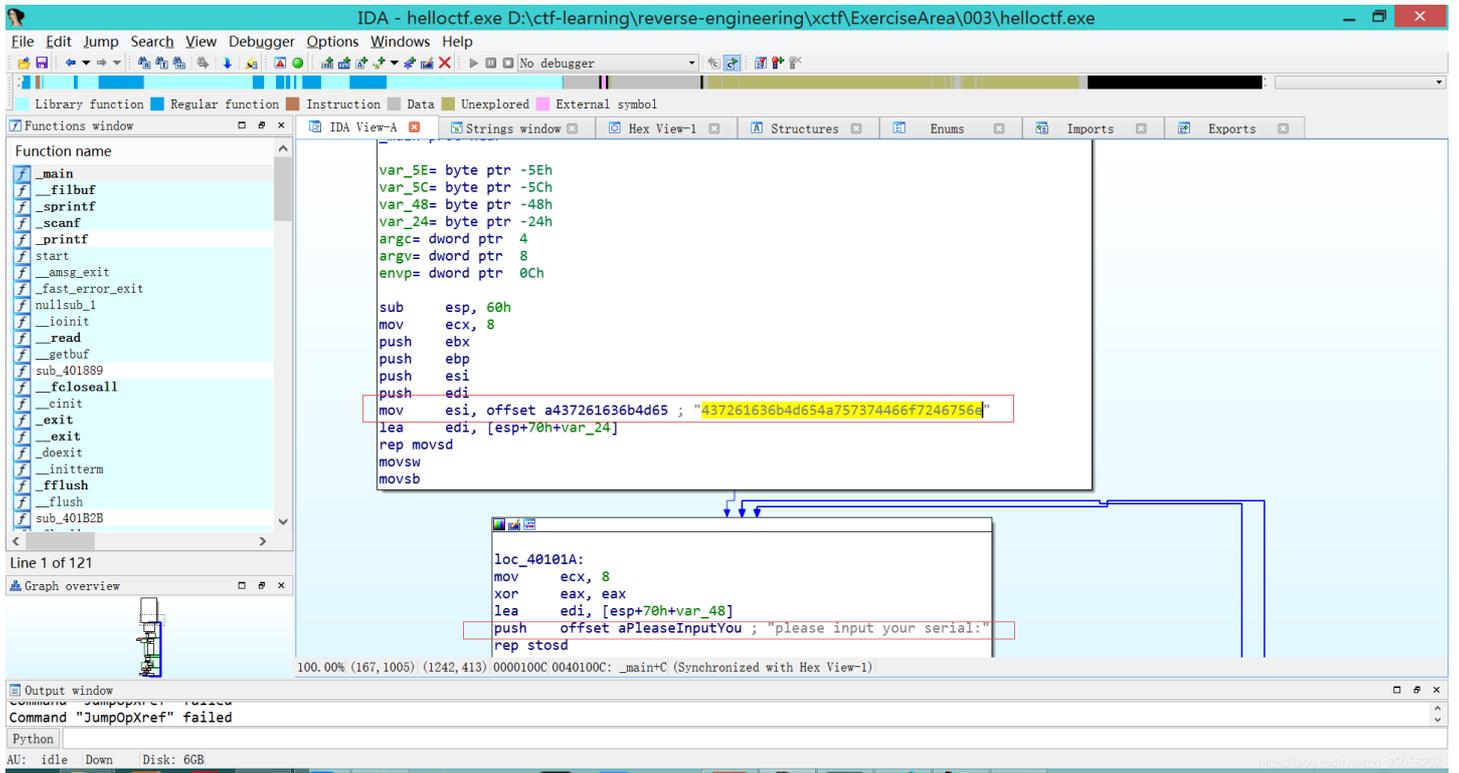
我们还是从字符串 `please input your serial:` 入手。用IDA打开helloctf.exe, `Shift+F12`, 显示在该二进制文件中的所有字符串。在顶部导航栏中: `Search` → `Search`, 输入字符串 `please input your serial:`, 然后双击跳转



再双击，跳到引用该字符串的地方。



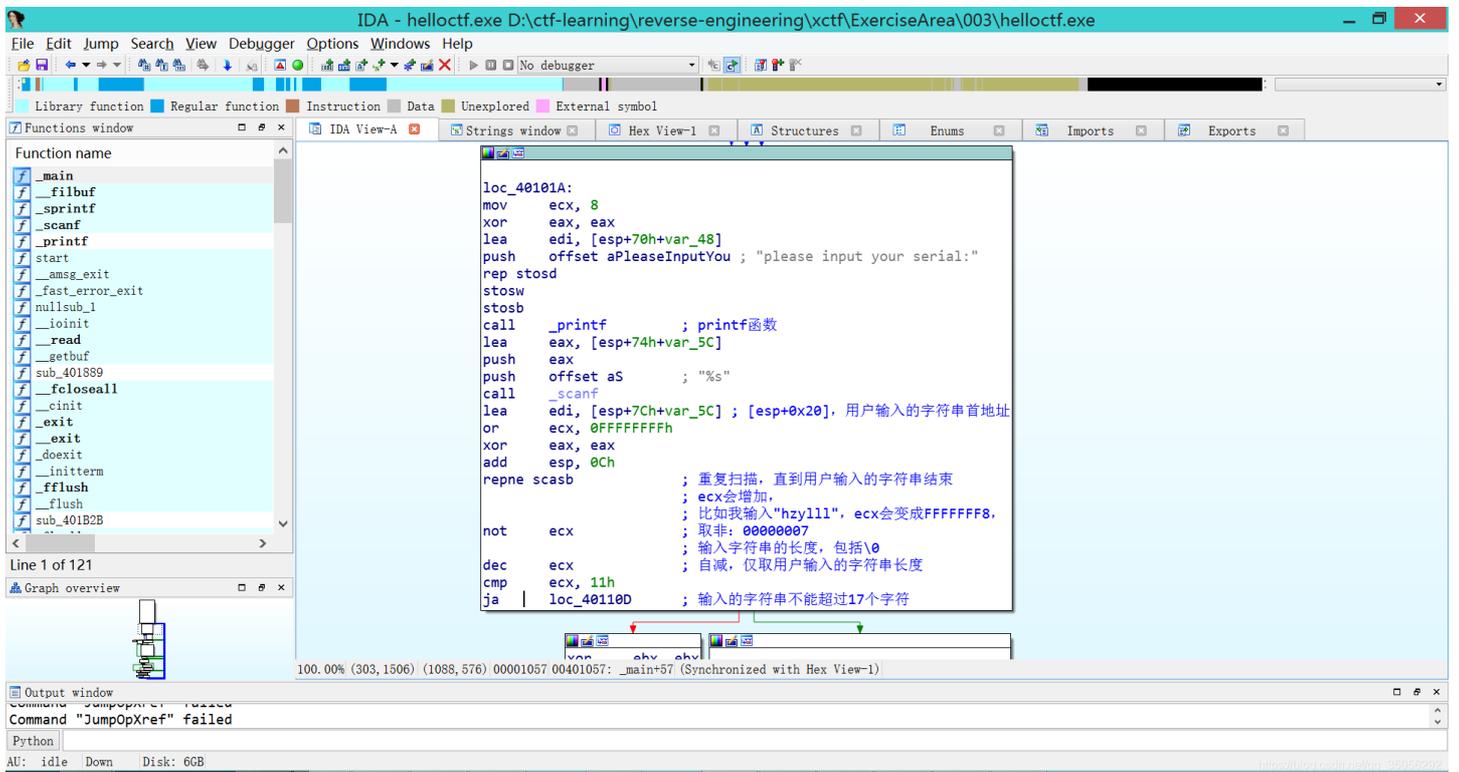
可以看到是在main中引用的



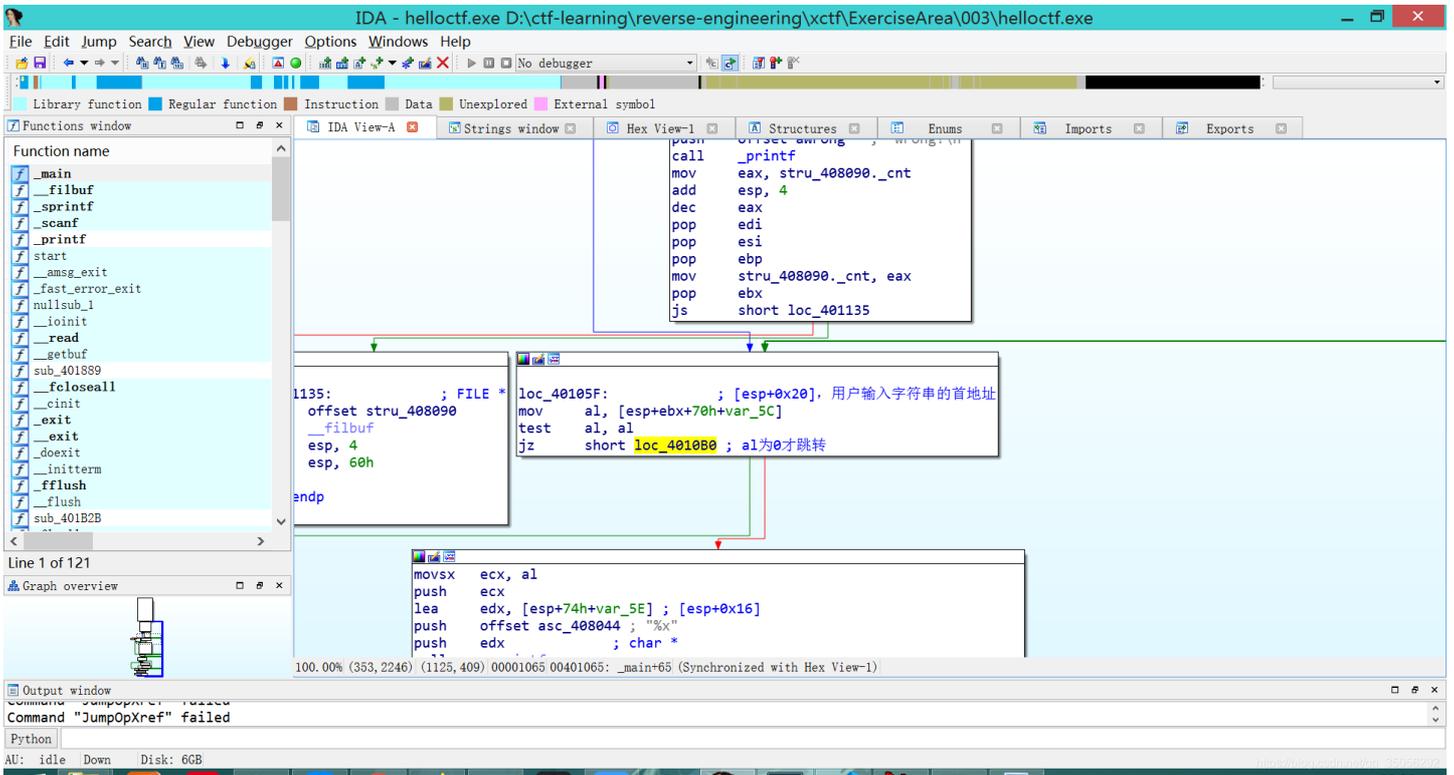
并且可以看到，在main函数的开始，将字符串 437261636b4d654a757374466f7246756e 赋值给了寄存器esi

## 1.2 具体基本块的分析

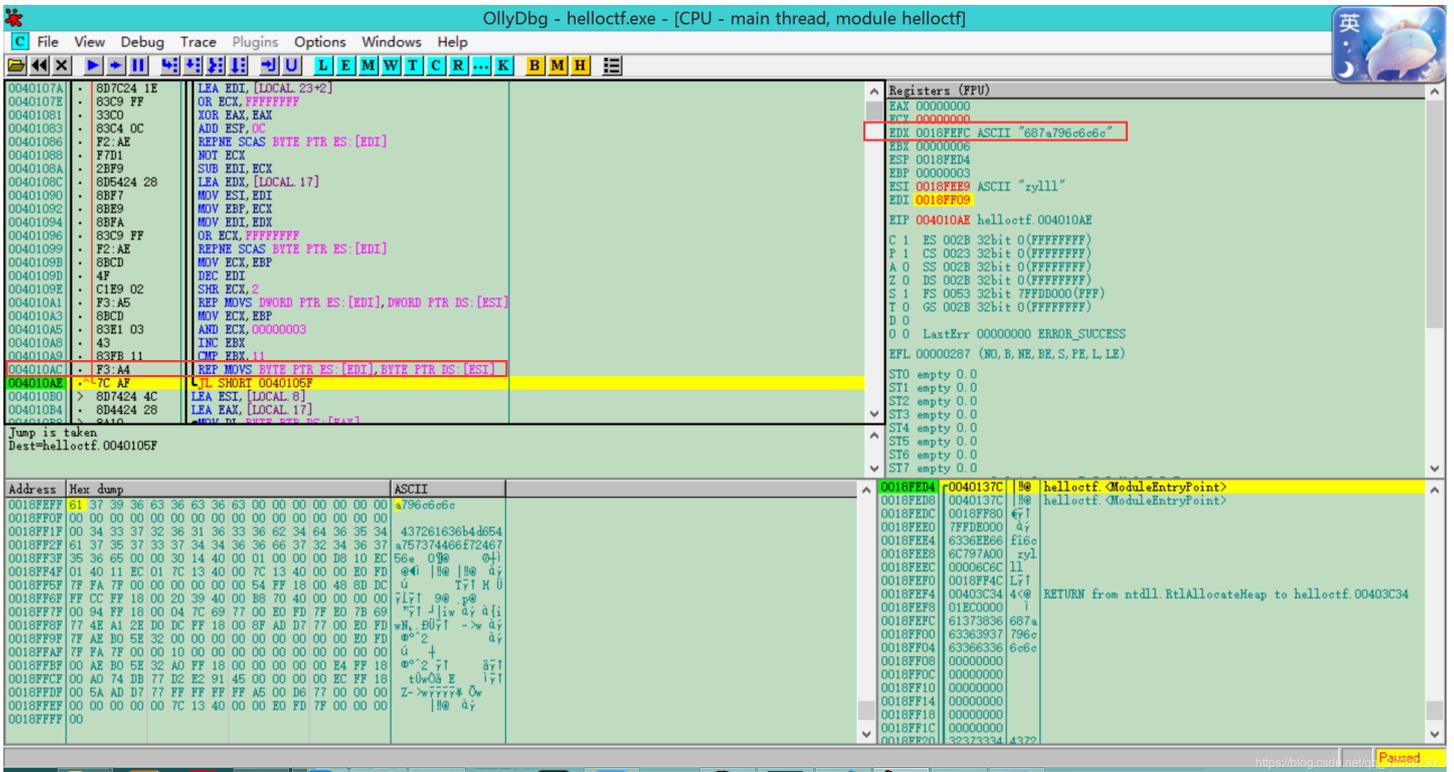
用Ollydbg来运行helloctf.exe。可以看到，地址0x40101A-0x401057是读取用户的输入，并对输入字符串的长度进行限制。



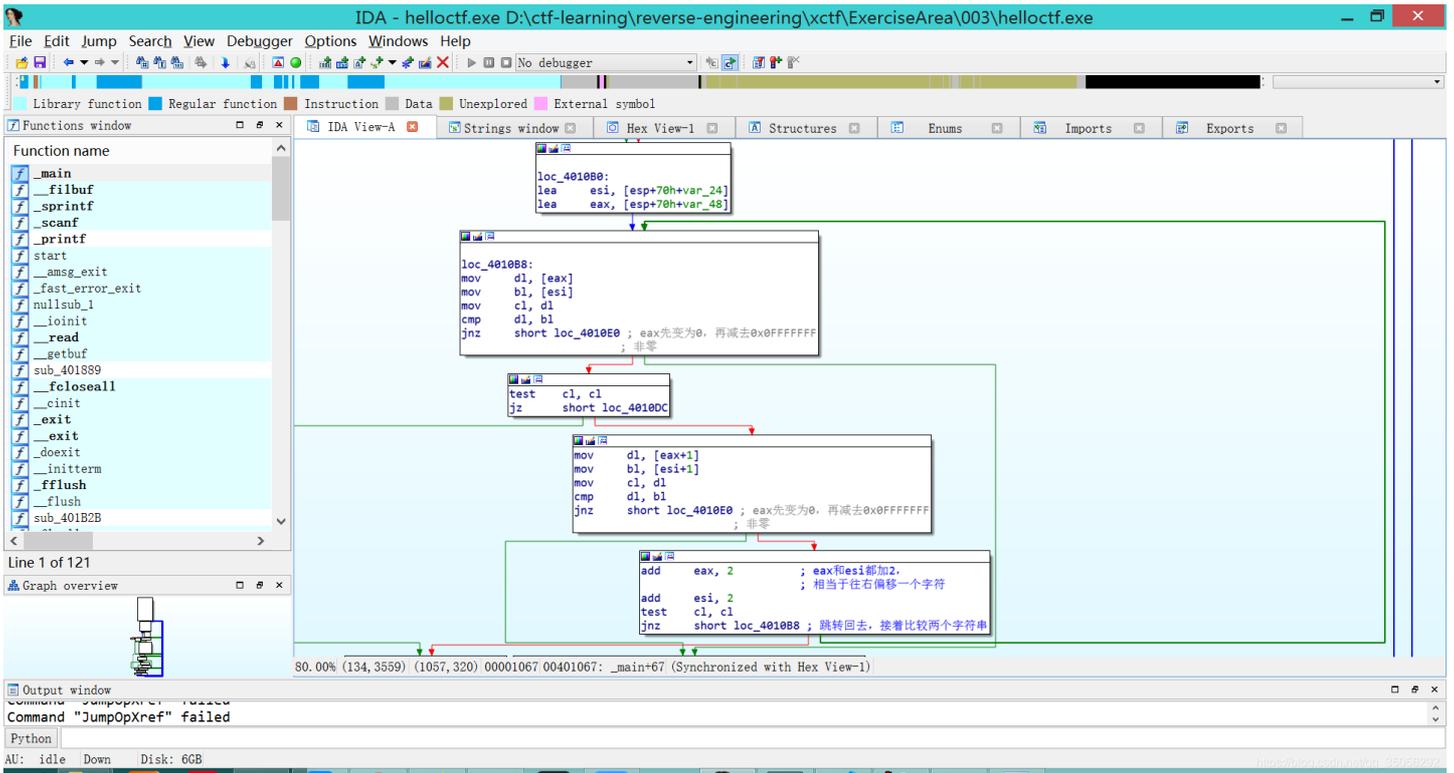
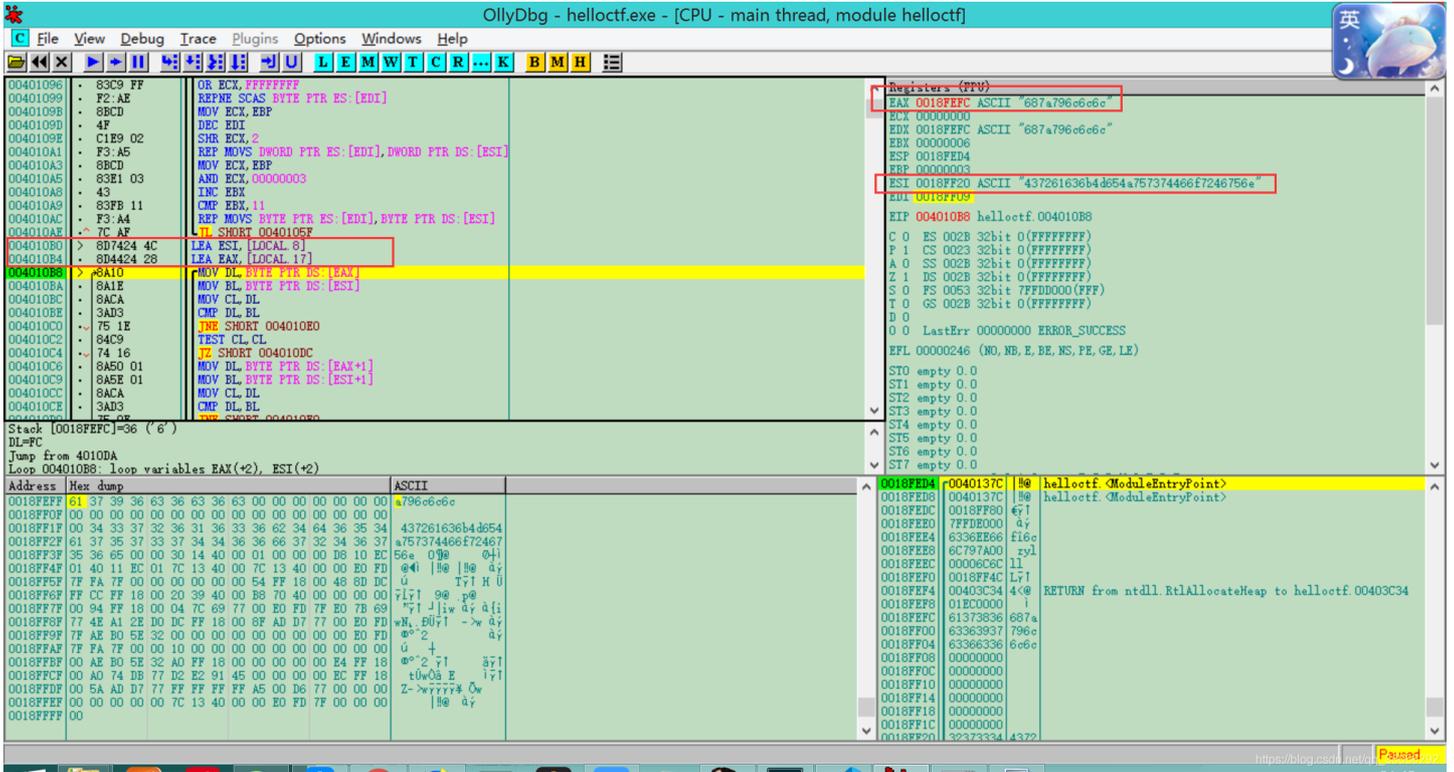
地址0x40105F将用户输入字符串的第一个字符赋值给了寄存器al，也就是寄存器eax的低八位。接下来，如果al保存的值为0则直接跳到与字符串 437261636b4d654a757374466f7246756e 比较的基本块。显然不符合要求，因此第一个字符不能为0



然后是最主要的部分，地址0x401067开始，对于用户输入的字符串，在循环中，将每个字符对应的十六进制数拼接到寄存器edx中保存，比如我输入的是 `hzylll`，那么得到的结果是 `687a796c6c6c`



从地址0x4010B0开始，让上面循环中得到的十六进制字符串跟一开始的字符串 `437261636b4d654a757374466f7246756e` 进行比较，二者一致才输出 `success` 的字样



结论：分析到这里，题目的意图很明了，给定一个字符串 437261636b4d654a757374466f7246756e，你的输入转成16进制字符串以后必须跟它一样。只要把代码中给的字符串转成ASCII码形式即可

解密脚本：

```
# -*- coding:utf-8 -*-
```

```
import binascii
```

```
src_str = '437261636b4d654a7573744466f7246756e'
```

```
res = binascii.a2b_hex(src_str)
```

```
print(res)
```

脚本运行结果为: CrackMeJustForFun

### 1.3 结果

输出 **success!** 信息, 说明拿到了flag

```
cmd - helloctf.exe
振洋@LENOVO-HZY D:\ctf-learning\reverse-engineering\xctf\ExerciseArea\003
$ helloctf.exe
please input your serial:abcdefg
wrong!
please input your serial:abc
wrong!
please input your serial:CrackMeJustForFun
success!
please input your serial:CrackMeJustForFun
success!
please input your serial:
helloctf.exe*[32]:7336
« 190108[64] 1/1 [+] NUM PRI↑ 80x25 (26.12) 50V 9252 100%
Net: 1/4 | log: osdn.net | qq: 36056292
```