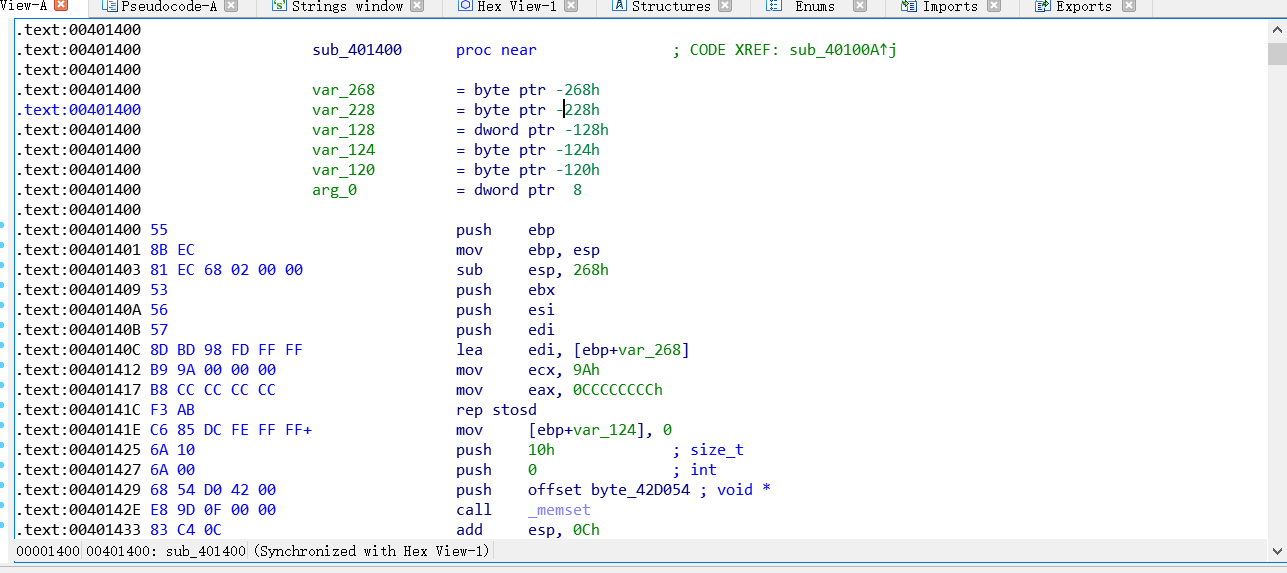
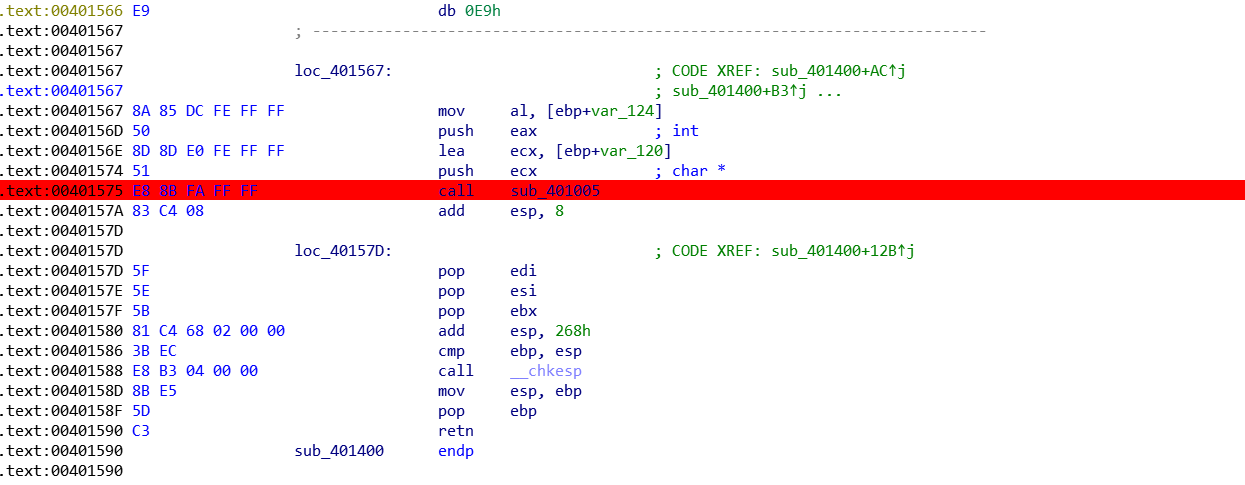
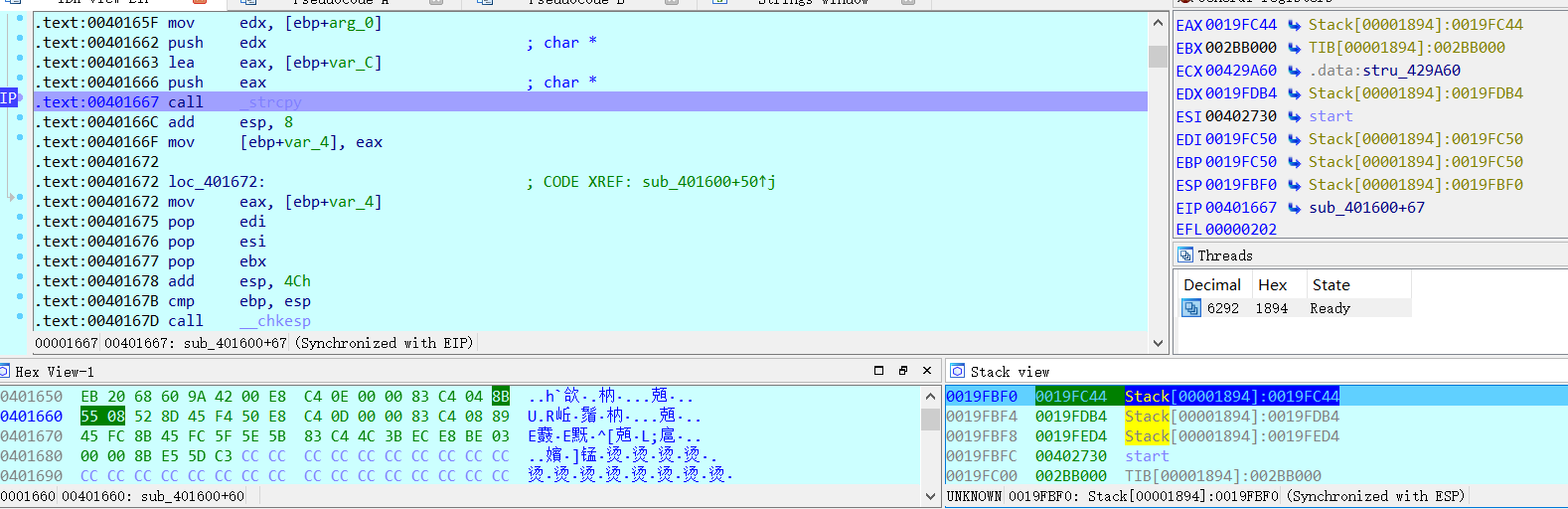
首先解决“花指令”的问题，让IDA正确分析汇编代码，并将代码段定义为函数。



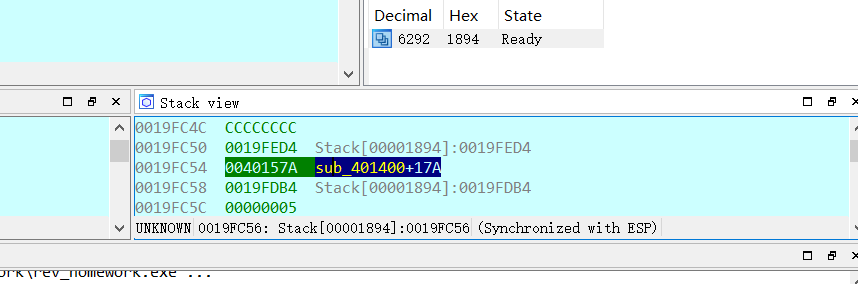
接下来寻找溢出点，在进入子函数处设置断点，调试跟踪。



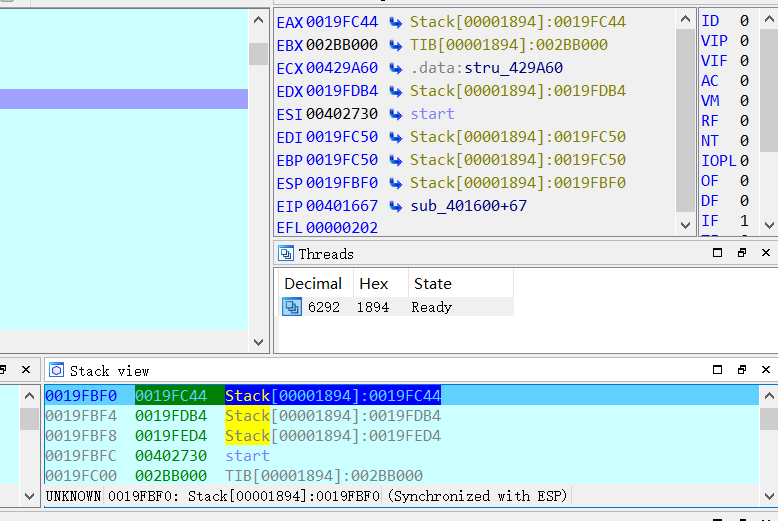
跟踪到strcpy处，观察堆栈。



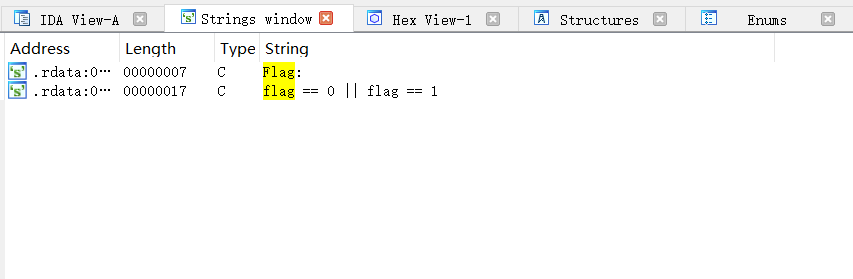
函数返回地址0x0040157A存储在0x0019FC54处。



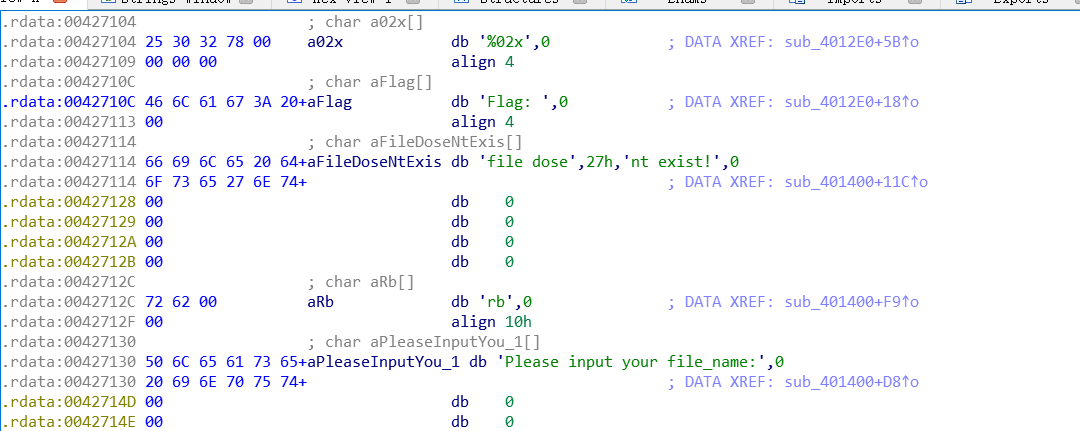
strcpy函数的复制起始地址存放在栈顶，为0x0019FC44。



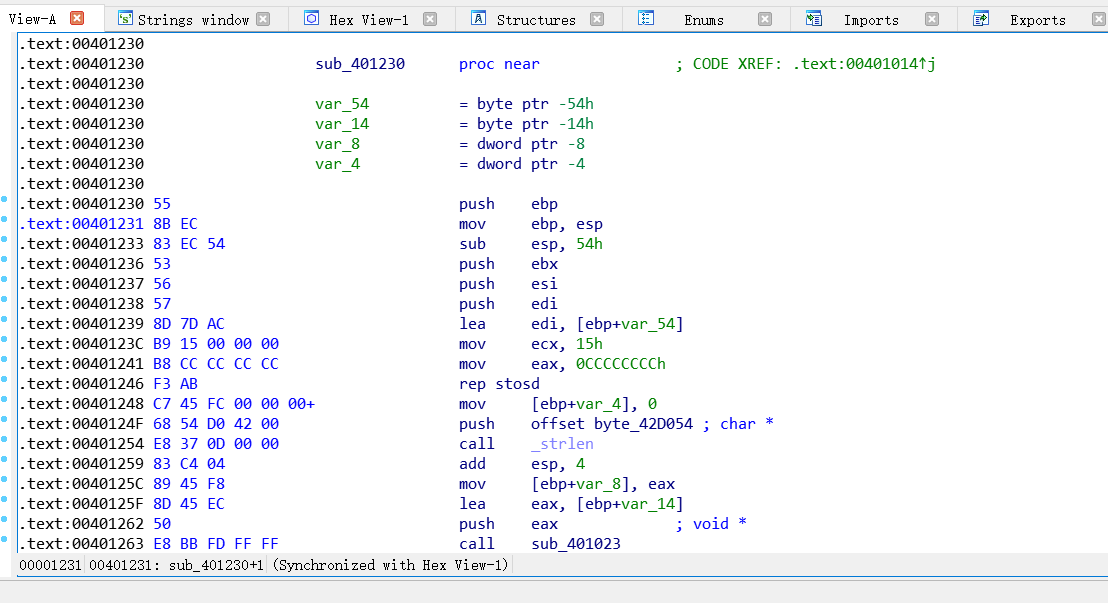
接着寻找Success、flag等字符串，success无法找到，可能是动态生成的原因，但是可以找到Flag字符串。



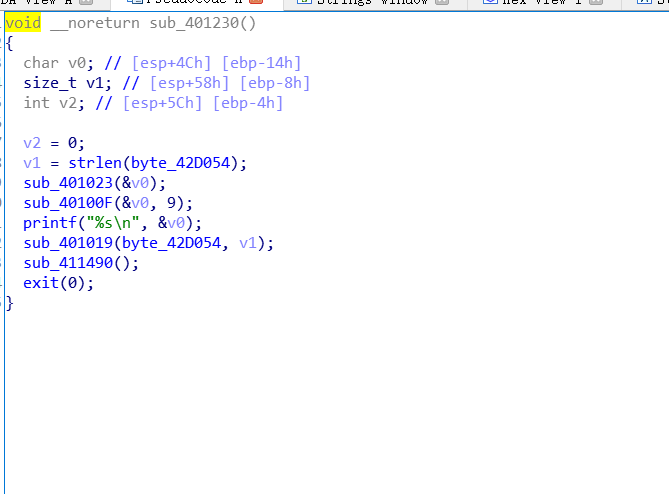
选择第一个Flag字符串，不断向上追溯。



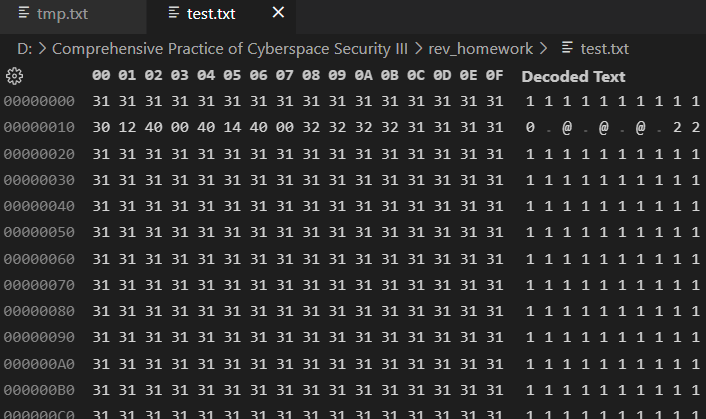
定位到需要调用的代码段，并将其定义为函数。



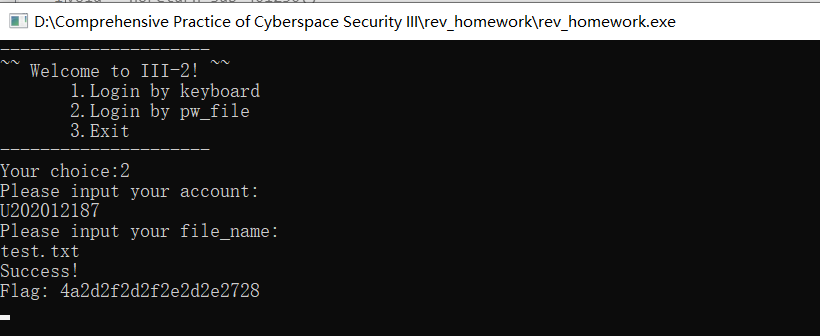
反汇编分析，具有打印字符串操作，并且调用了exit函数。经过分析，其为需要调用的子函数，函数地址为0x00401230。



经过计算，将0x00401230填充在发送数据的0x10~0x13字节处。



运行程序，用户名为U202012187，发送test.txt文件，攻击成功。



得到Flag为：4a2d2f2d2f2e2d2e2728。