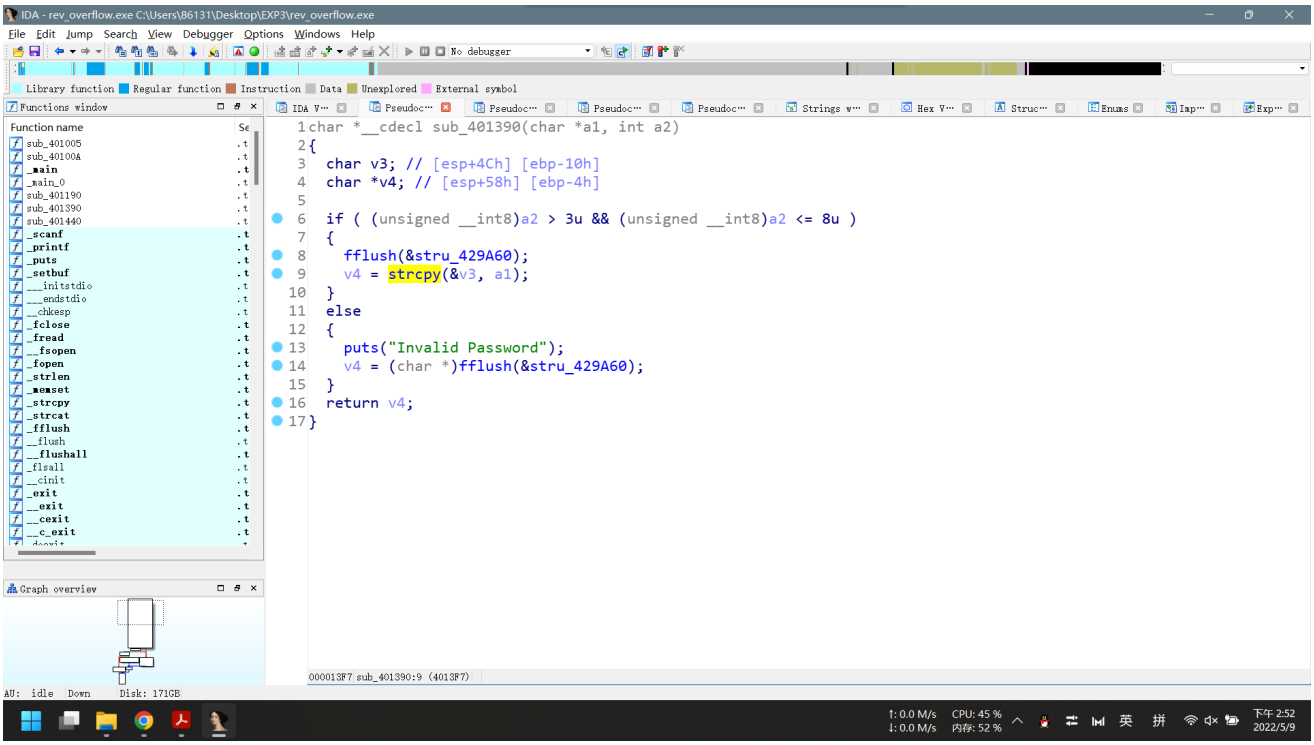
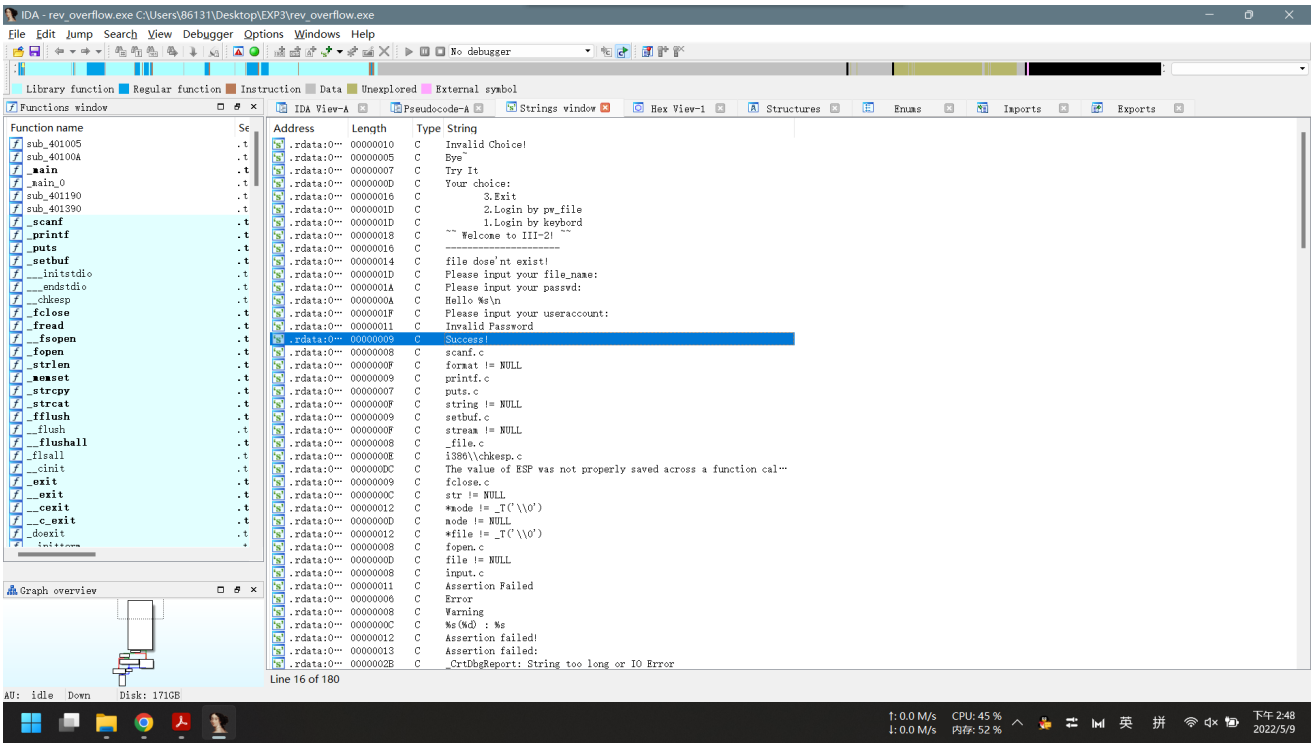
1. 程序漏洞位置

- strcpy 前 LOBYTE(v1) = v5; 结合 (unsigned __int8)a2 > 3u && (unsigned __int8)a2 <= 8u 使得程序可能发生整数溢出：

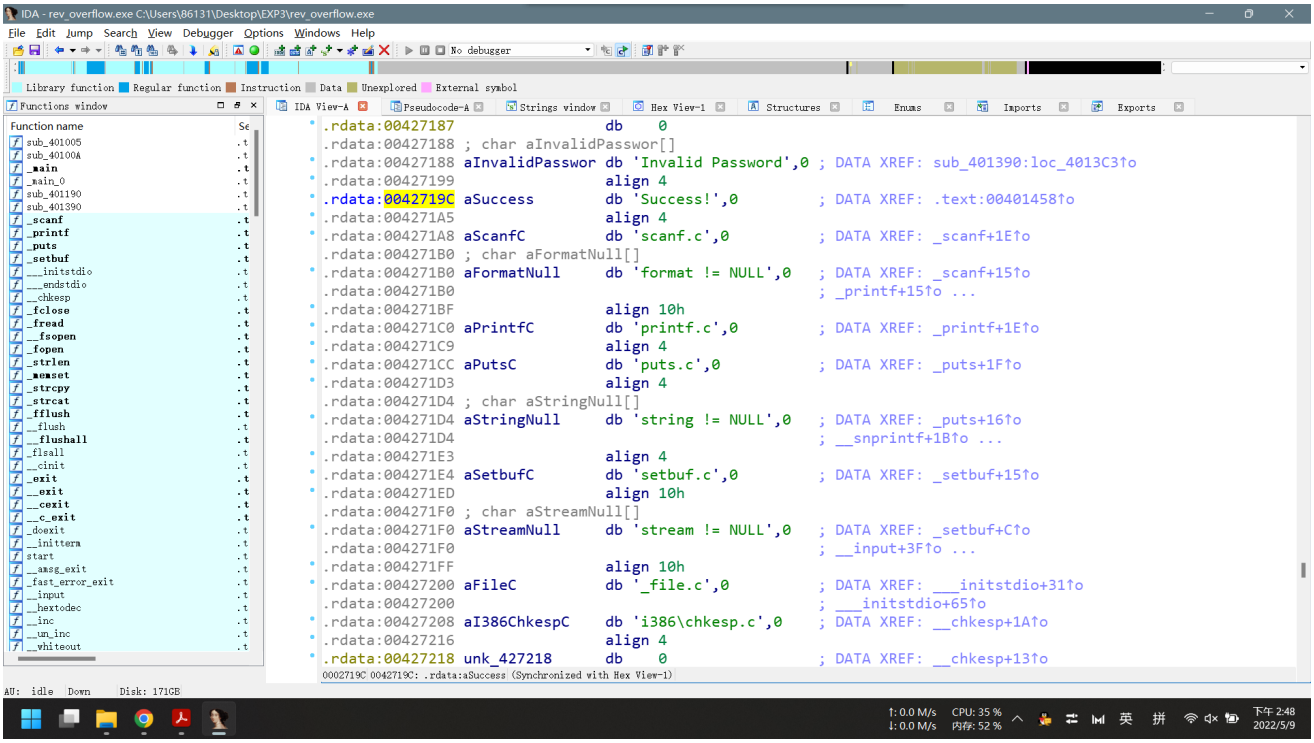


2. 包含 Success! 提示的函数偏移地址为 0x00401440

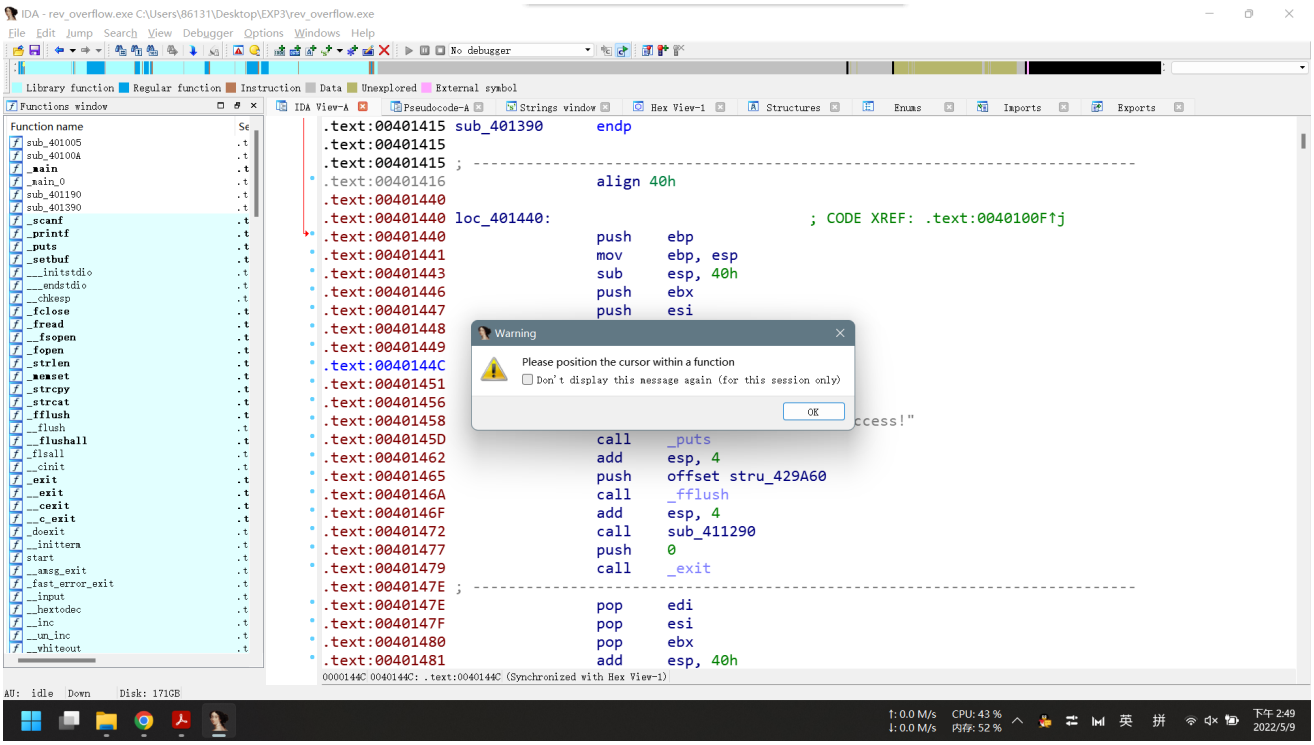
- 在字符串表中寻找目标字符串 Success! ：



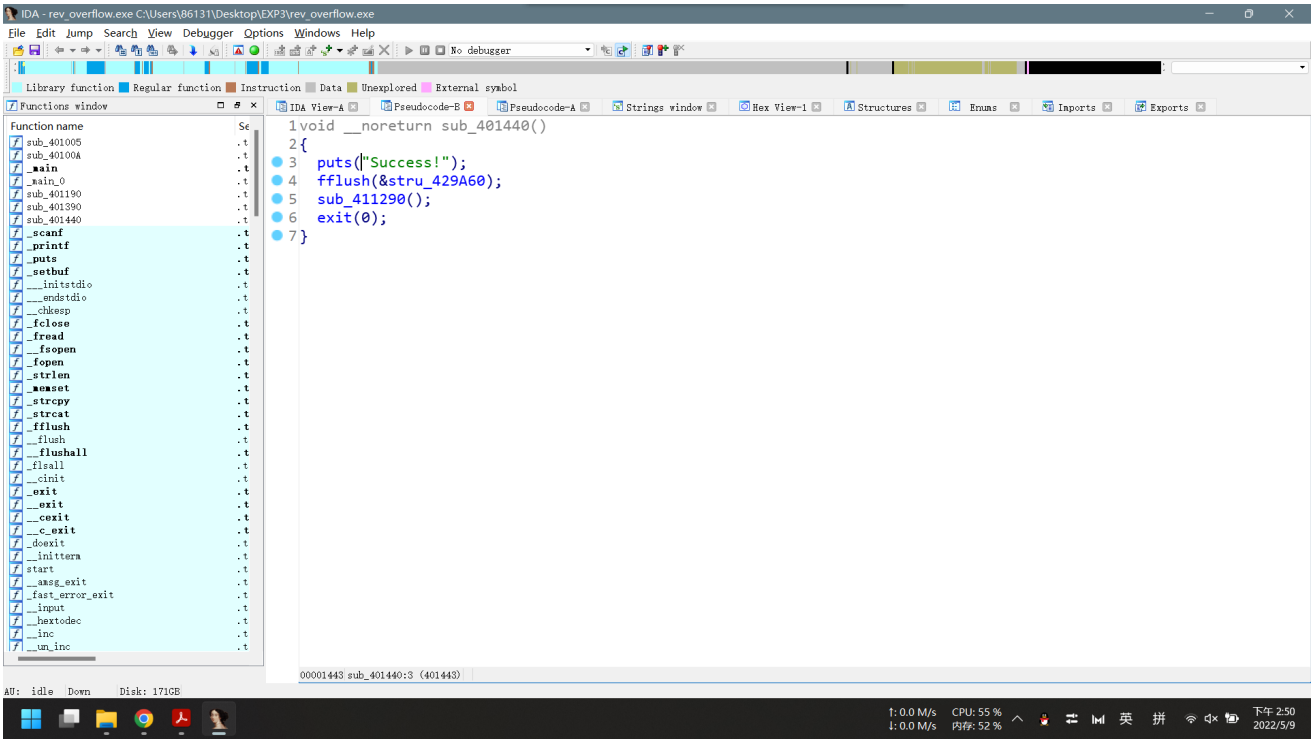
- 找到目标字符串在内存中的位置，并根据引用找到使用它的程序的地址：



- 使用该字符串的函数的偏移地址为 `0x00401440`，手动将其反编译：

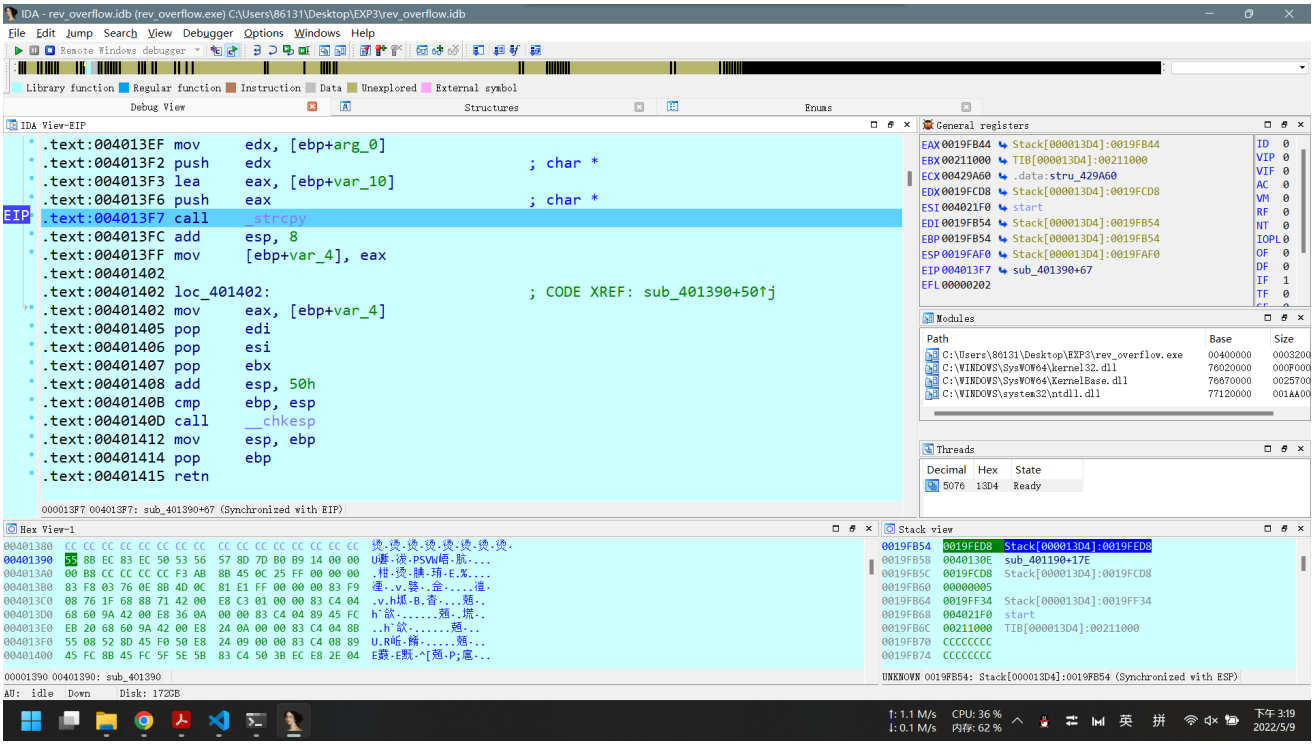


- 反编译结果：

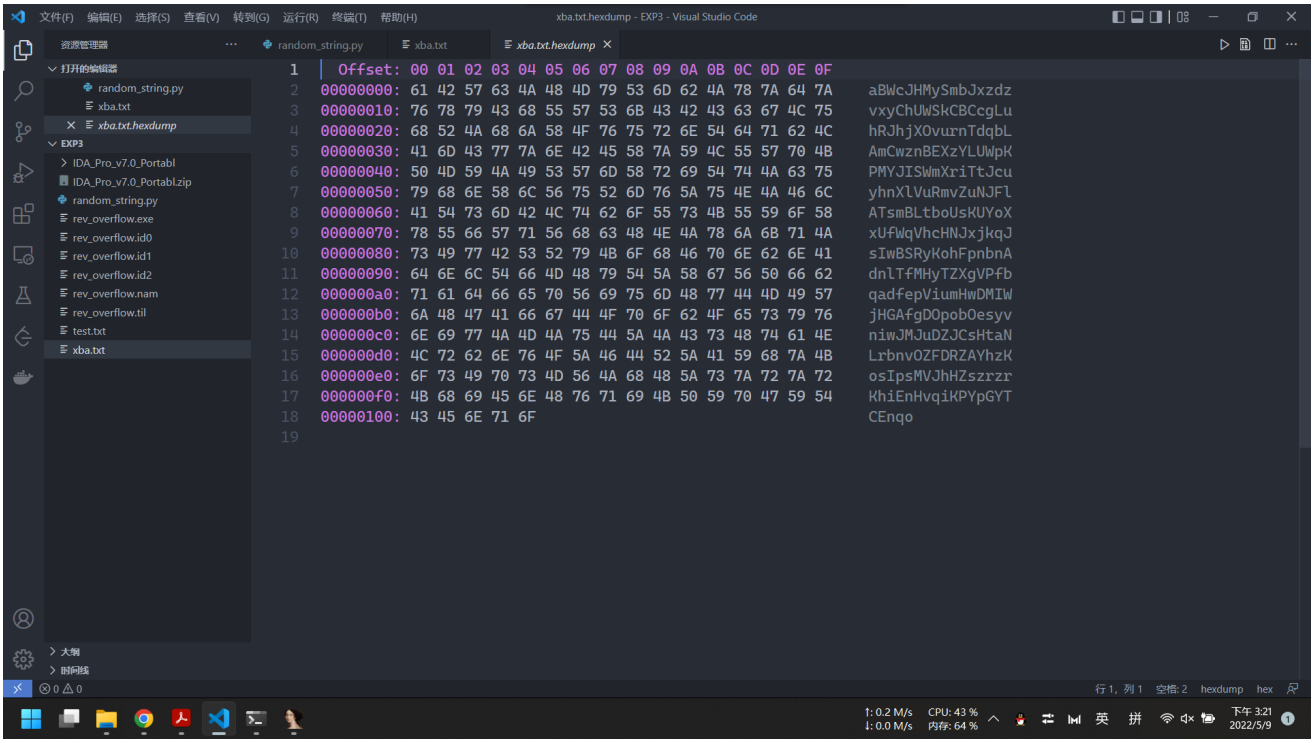


3. 构建二进制输入文件

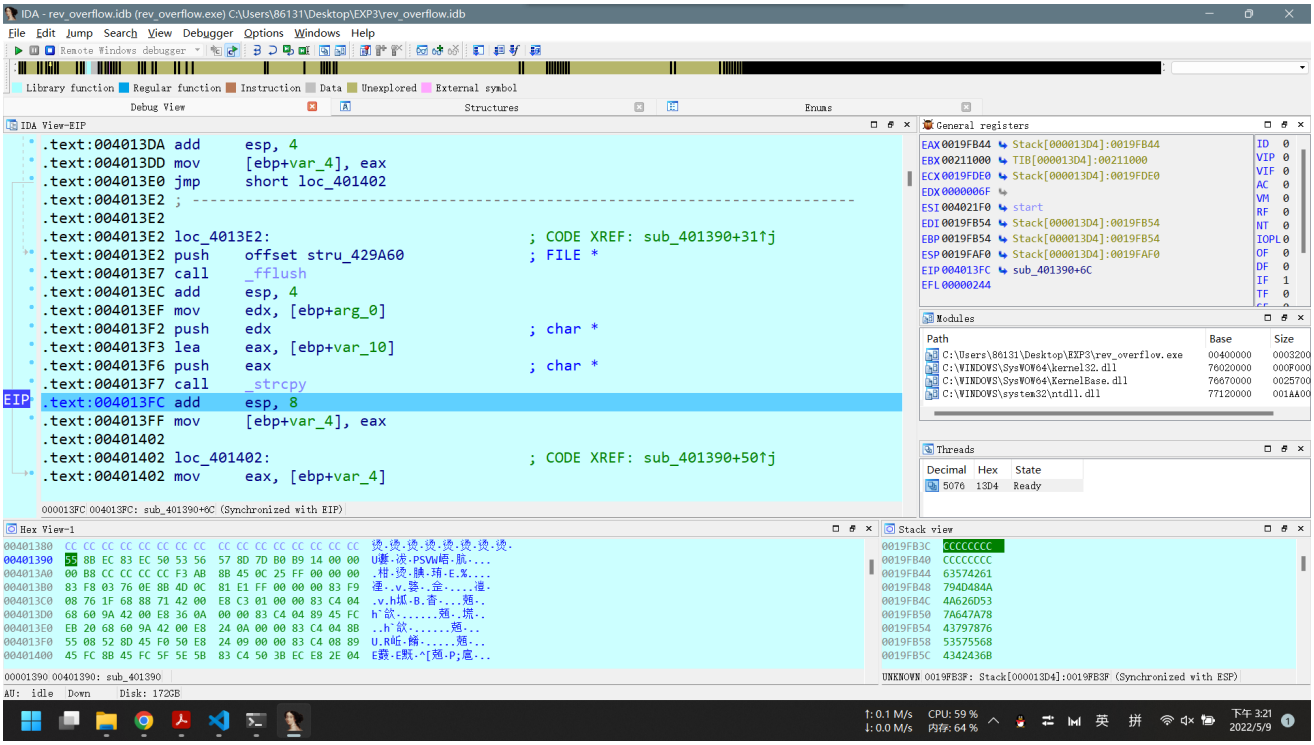
- 动态调试，在 `strcpy` 函数执行前，可以看到栈中 `0x0019FB58` 的位置存放着返回地址：



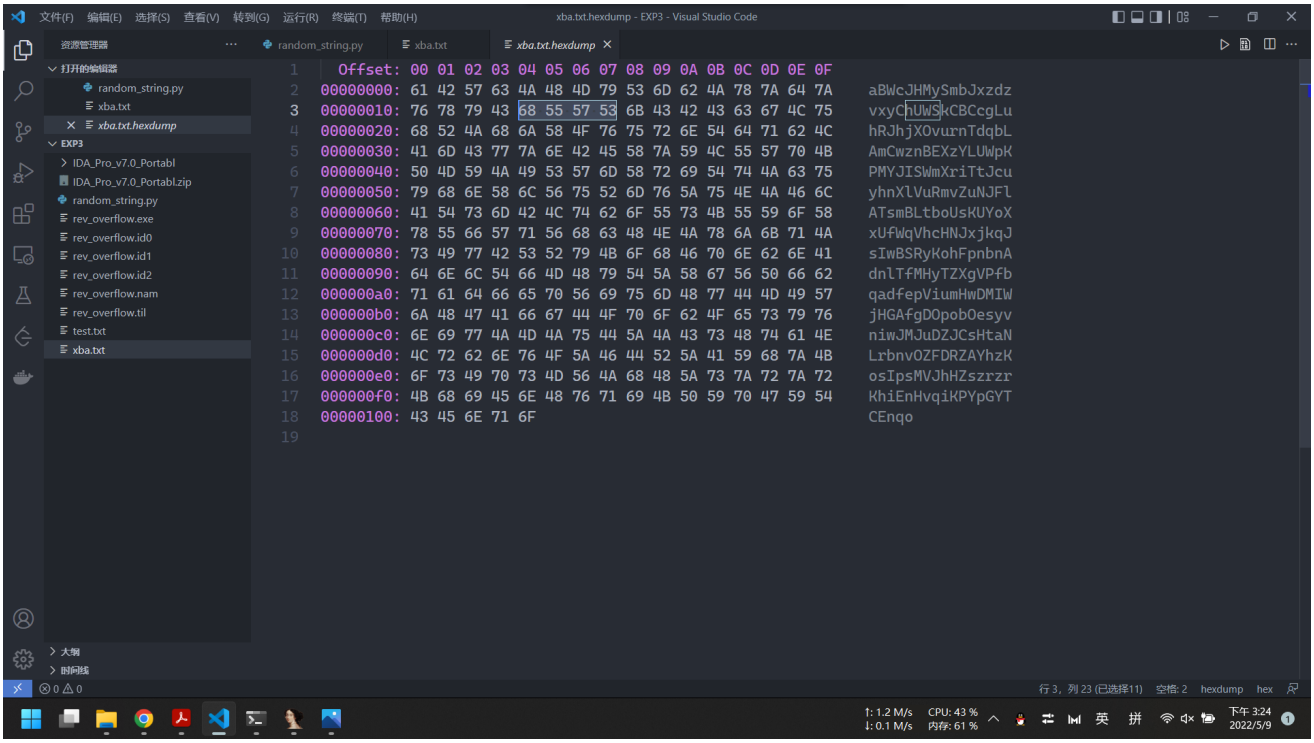
- 使用以下随机生成的长度为 `256 + 5` 字符串进行测试：



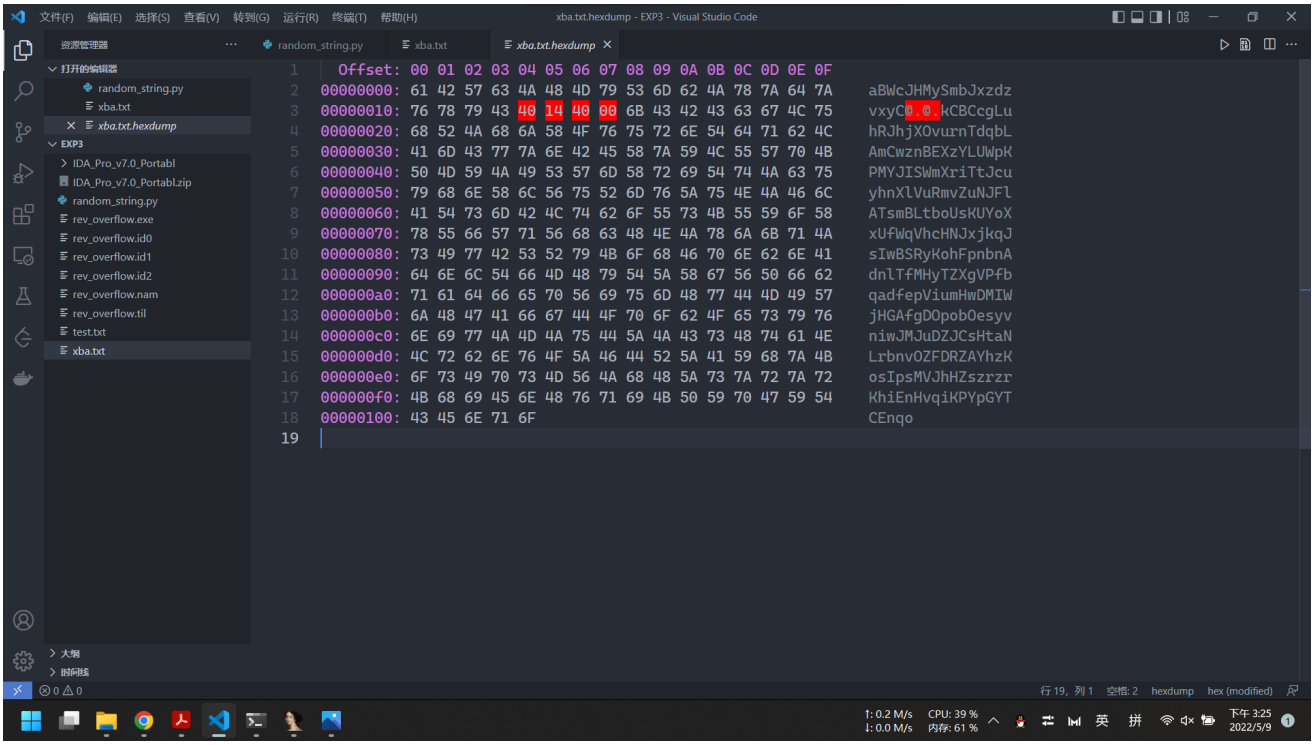
- 返回地址的位置 `0x0019FB58` 被替换为 `0x53575568`：



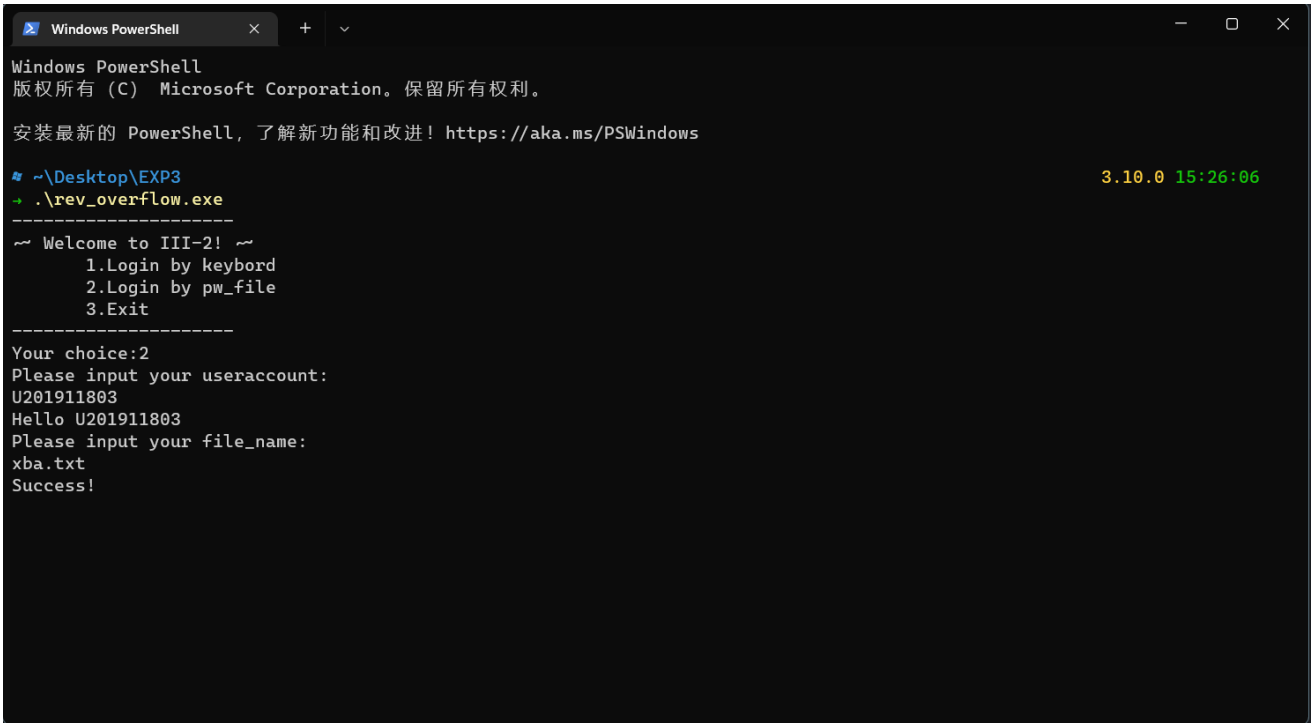
- 在构造的字符串文件中搜索这四个字符，可以找到需要修改的位置（也可以根据老师使用的数偏移地址的方式确定要修改的位置）：



- 将其修改为输出`Success!`的函数的地址，至此二进制输入文件`xba.txt`构造完成：



4. 测试程序，能够提示`Success!`


Windows PowerShell
Windows PowerShell
版权所有 (C) Microsoft Corporation。保留所有权利。
安装最新的 PowerShell，了解新功能和改进！ https://aka.ms/PSWindows
~\Desktop\EXP3
3.10.0 15:26:06
.\rev_overflow.exe
~~ Welcome to III-2! ~~
1.Login by keybord
2.Login by pw_file
3.Exit
Your choice:2
Please input your useraccount:
U201911803
Hello U201911803
Please input your file_name:
xba.txt
Success!