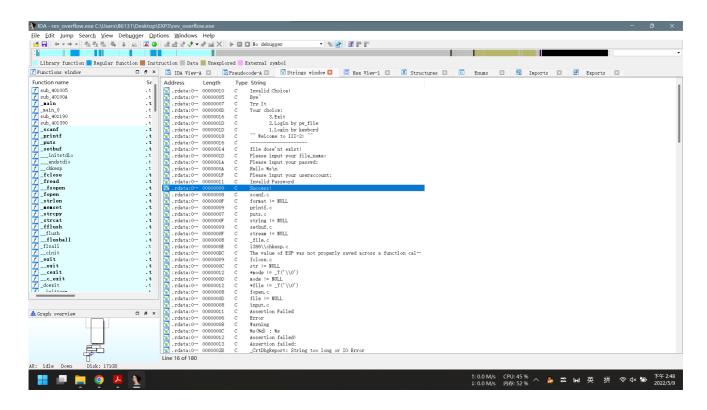
1. 程序漏洞位置

■ 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:

```
TIDA - rev_overflow.exe C:\Users\86131\Desktop\EXP3\rev_overflow.exe
 File Edit Jump Search View Debugger Options Windows Help
    ▼ 16 😝 📝 🔐 😭
        🖪 Pseudoc… 🗵 👿 Strings w… 🗵 🔘 Hex V… 🗵 🖪 Struc… 🗈 🖽 Enums 🗈 📆 Imp… 🗈 👺 Exp… 🗈
 Function name
| F sub_401005 |
| F sub_401006 |
| F sub_401007 |
| F sub_401190 |
| F sub_401190 |
| F sub_401190 |
| F sub_40140 |
| F sub_40
                                                                                                                                                      char v3; // [esp+4Ch] [ebp-10h]
char *v4; // [esp+58h] [ebp-4h]
                                                                                                                                                     if ( (unsigned __int8)a2 > 3u && (unsigned __int8)a2 <= 8u )
                                                                                                                            • 8
• 9
                                                                                                                                                               fflush(&stru_429A60);
                                                                                                                                                               v4 = \frac{1}{\text{strcpy}}(\sqrt[8]{8}v3, a1);
                                                                                                                                    11 else
                                                                                                                                     12 {
                                                                                                                            13
14
15 }
                                                                                                                                                             puts("Invalid Password");
                                                                                                                                                                v4 = (char *)fflush(&stru_429A60);
                                                                                                                                                       return v4:
                                                                                                  □ 8 ×
A Graph overview
                                                                                                                                                000013F7 sub_401390:9 (4013F7)
                                                                                                                                                                                                                                                                                                                                                                                                                                  1: 0.0 M/s CPU: 45 % ↑ ↓ ★ Iml 英 拼 常 Ф ▼ ■
```

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!:



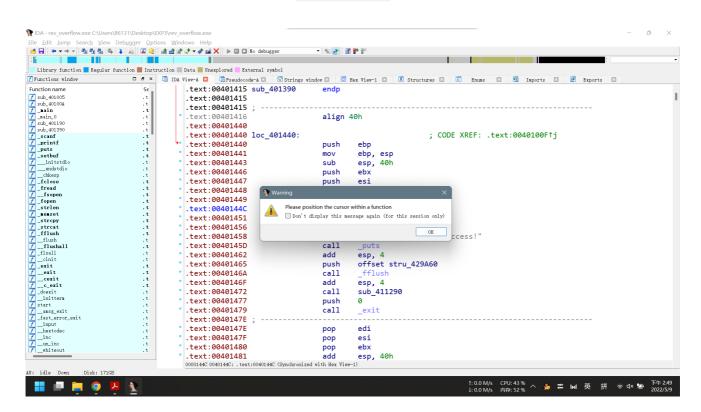
■ 找到目标字符串在内存中的位置,并根据引用找到使用它的程序的地址:

```
TIDA - rev_overflow.exe C:\Users\86131\Desktop\EXP3\rev_overflow.exe
Library function Regular function instruction Data Unexplored External symbol Functions window D X D IDA View-A N Description
                                                                                                                                  code-A 🗵 🕏 Strings window 🗔 🖸 Hex View-1 🗵 🖪 Structures 🚨 🖽 Enuas 🖾 📆 Imports 🚨 🗭 Exports 🗵
 Function name
                                                                                           .rdata:00427187
                                                                                                                                                                                 db
 | sub_401005 | sub_401005 | sub_401005 | sub_401005 | sub_401000 | sub_401000 | sub_401300 | seanf | puts | setbuf | seanf | puts | setbuf | seanf | puts | setbuf | seanf | s
                                                                                              .rdata:00427188; char aInvalidPasswor[]
.rdata:00427188 aInvalidPasswor db 'Invalid Password',0; DATA XREF: sub_401390:loc_4013C3fo
                                                                                              .rdata:00427199
.rdata:0042719C aSuccess
                                                                                                                                                                                  align 4
                                                                                                                                                                                                                                               ; DATA XREF: .text:004014581o
                                                                                                                                                                                 db 'Success!',0
                                                                                              .rdata:004271A5
.rdata:004271A8 aScanfC
                                                                                                                                                                                  align 4
                                                                                                                                                                                            'scanf.c',0
                                                                                                                                                                                                                                               ; DATA XREF: _scanf+1E1o
                                                                                                                                                                                 db
                                                                                              ; DATA XREF: _scanf+15↑o
; _printf+15↑o ...
                                                                                               .rdata:004271B0
                                                                                               .rdata:004271BF
                                                                                                                                                                                  align 10h
                                                                                           .rdata:004271C0 aPrintfC
                                                                                                                                                                                 db 'printf.c',0
align 4
                                                                                                                                                                                                                                                ; DATA XREF: _printf+1E1o
                                                                                              .rdata:004271C9
                                                                                          *.rdata:0042/1CC arucoc

*.rdata:0042/1D3 align 4
.rdata:004271D4 ; char aStringNull[]

*.taraaaa771D4 aStringNull db 'string != NULL',0
                                                                                              .rdata:004271CC aPutsC
                                                                                                                                                                                 db 'puts.c'.0
                                                                                                                                                                                                                                               : DATA XREF: _puts+1F1o
                                                                                          *.rdata:004271D4 aStringNull
.rdata:004271D4
*.rdata:004271D4
                                                                                                                                                                                                                                                ; DATA XREF: _puts+16↑o
; __snprintf+1B↑o ...
                                                                                                                                                                                                                                              ; DATA XREF:
                                                                                                                                                                                 align 4
                                                                                          .rdata:004271E4 aSetbufC
                                                                                                                                                                                            'setbuf.c',0
                                                                                                                                                                                                                                                ; DATA XREF: _setbuf+15↑o
                                                                                          .rdata:004271ED
                                                                                             .rdata:004271ED .rdata:004271E0 ; char aStreamNull[] .rdata:004271E0 aStreamNull db 'stream != NULL',0
                                                                                                                                                                                  align 10h
                                                                                          · .rdata:004271F0 aStreamNull
                                                                                                                                                                                                                                                 ; DATA XREF: _setbuf+Cfo
; __input+3Ffo ...
                                                                                                                                                                                                                                                ; DATA XREF:
                                                                                          .rdata:004271F0
                                                                                                                                                                                 align 10h
db '_file.c',0
                                                                                              .rdata:004271FF
                                                                                                                                                                                                                                                 ; DATA XREF: __initstdio+31fo
; __initstdio+65fo
; DATA XREF: __chkesp+1Afo
                                                                                          • .rdata:00427200 aFileC
                                                                                              .rdata:00427200
                                                                                          .rdata:00427208 aI386ChkespC
.rdata:00427216
                                                                                                                                                                                 db 'i386\chkesp.c',0
                                                                                                                                                                                 align 4
                                                                                                                                                              18 db 0
                                                                                               .rdata:00427218 unk 427218
                                                                                                                                                                                                                                                  ; DATA XREF: chkesp+131c
                                                                                              0002719C 0042719C: .rdata:aSuccess (Sy
     1:0.0 M/s CPU:35 % へ 💃 君 📶 英 拼 🛜 Ф× 🖆 下午2:48
1:0.0 M/s 内存:52 % ヘ 💃 君 📶 英 拼 🛜 Ф× 🐿 2022/5/9
```

■ 使用该字符串的函数的偏移地址为 0×00401440 , 手动将其反编译:

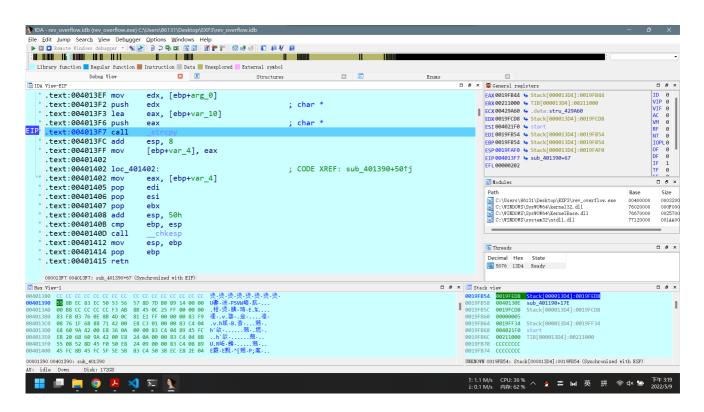


■ 反编译结果:

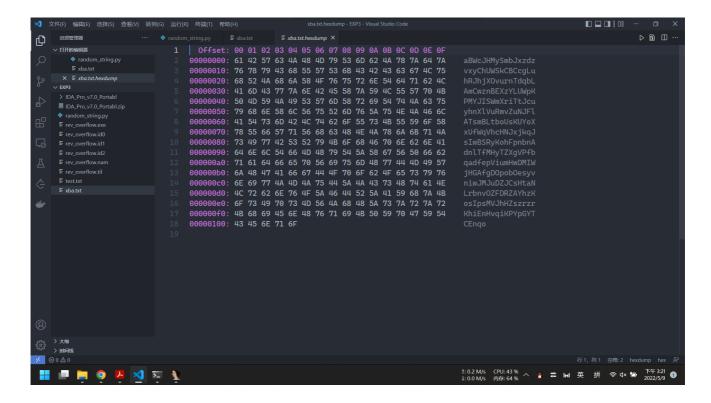
```
TIDA - rev_overflow.exe C:\Users\86131\Desktop\EXP3\rev_overflow.exe
   File Edit Jump Search View Debugger Options Windows Help
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         ▼ % (a) (ii) (iii) (iii
                             Library function Regular function Instruction Data Insert 
                                                                                                                                                                                                                                                                                                                                                   □ # × □ IDA View-A □ □ Pseudocode-B ☑
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           Pseudocode-A □ Strings window □ OHex View-1 □ AStructures □ Emus □ Maports □ FExports □
                                                                                                                                                                                                                                                                                                                                                                                   Se . t . t . t . t . t . t . t . t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                       lvoid __noreturn sub_401440()
         Function name
         | sub_401008 | sub_401008 | sub_401008 | sub_401004 | sain.0 | sub_401390 | sub_401390 | sub_401390 | sub_401440 | security | sector | sector | sector | sub_401440 | sector | sub_401440 | sector | sub_401440 | sector | sub_401390 | sub_401390 | sector | sub_401390 
                                                                                                                                                                                                                                                                                                                                                                                                                                                                           2 {
                                                                                                                                                                                                                                                                                                                                                                                                                                    2 {
3 puts(|"Success!");
4 fflush(&stru_429A60);
5 sub_411290();
6 exit(0);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        exit(0);
   f start
f __amsg_exit
f fast_error_exit
f __input
f __hextodec
f __inc
f __un_inc
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 00001443 sub_401440:3 (401443)
                         = • •
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        ↑:0.0 M/s CPU: 55 % へ 🐞 💤 🕪 英 拼 🛜 Ф× 🖆 下午 2:50 2022/5/9
```

3. 构建二进制输入文件

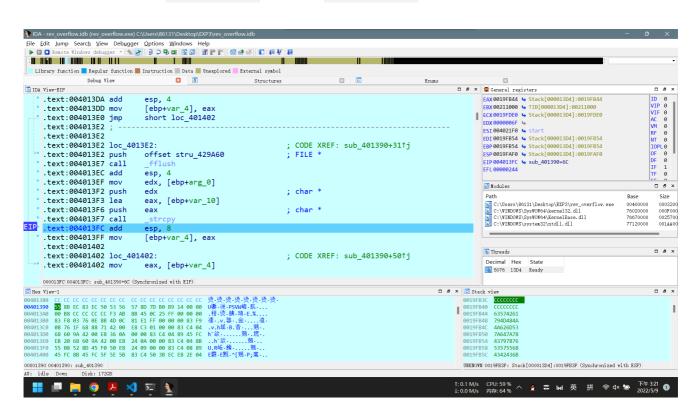
■ 动态调试,在 strcpy 函数执行前,可以看到栈中 0x0019FB58 的位置存放着返回地址:



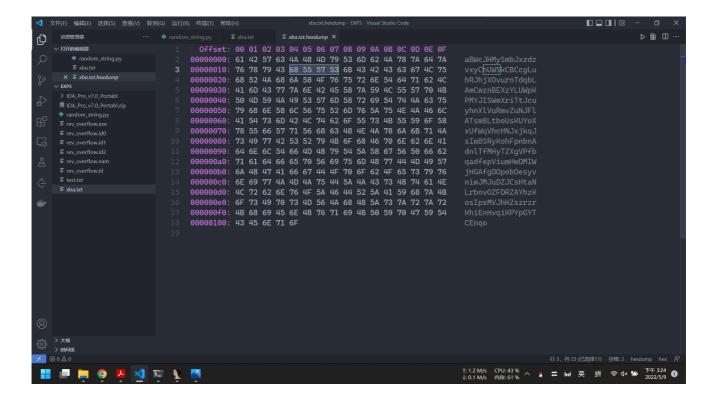
■ 使用以下随机生成的长度为 256 + 5 字符串进行测试:



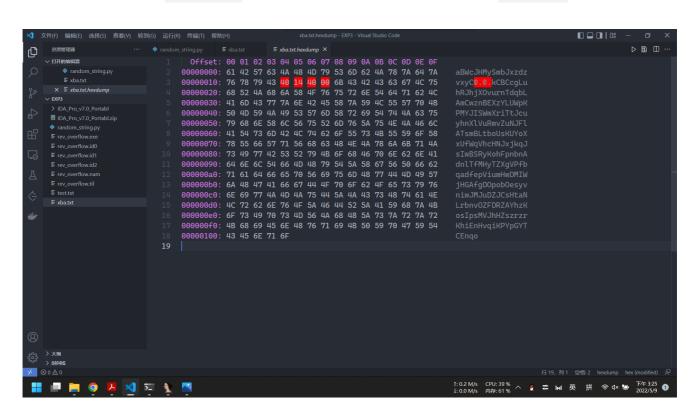
■ 返回地址的位置 0x0019FB58 被替换为 0x53575568:



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!

