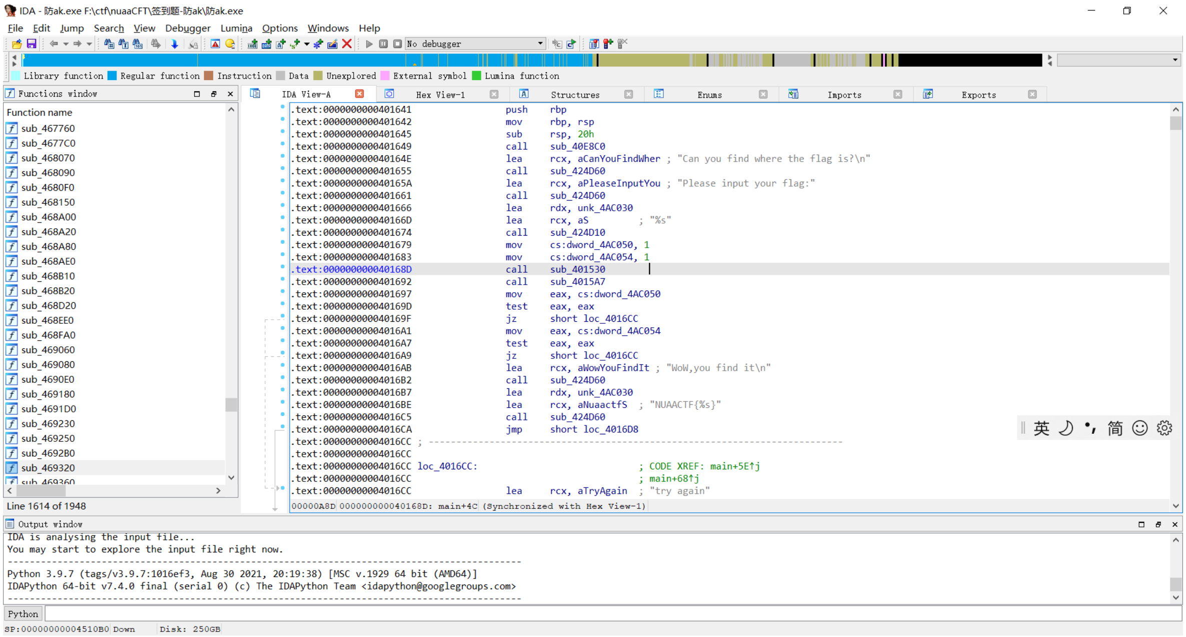
防ak

广受好评的送分题

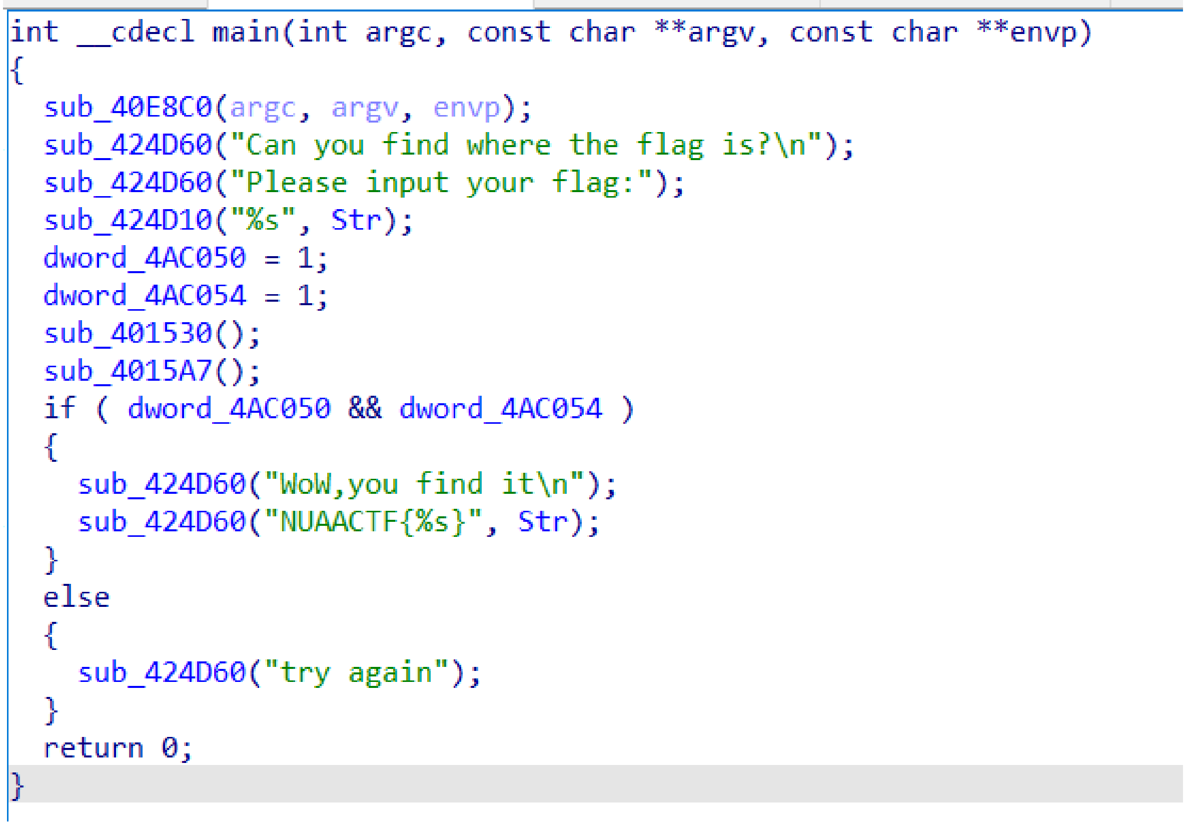
ida打开



```
.text:0000000000401641                 push    rbp
.text:0000000000401642                 mov     rbp, rsp
.text:0000000000401645                 sub     rsp, 20h
.text:0000000000401649                 call    sub_40E8C0
.text:000000000040164E                 lea     rcx, aCanYouFindWher ; "Can you find where the flag is?\n"
.text:0000000000401655                 call    sub_424D60
.text:000000000040165A                 lea     rcx, aPleaseInputYou ; "Please input your flag:"
.text:0000000000401661                 call    sub_424D60
.text:0000000000401666                 lea     rdx, unk_4AC030
.text:000000000040166D                 lea     rcx, aS         ; "%s"
.text:0000000000401674                 call    sub_424D10
.text:0000000000401679                 mov     cs:dword_4AC050, 1
.text:0000000000401683                 mov     cs:dword_4AC054, 1
.text:000000000040168D                 call    sub_401530
.text:0000000000401692                 call    sub_4015A7
.text:0000000000401697                 mov     eax, cs:dword_4AC050
.text:000000000040169D                 test    eax, eax
.text:000000000040169F                 jz      short loc_4016CC
.text:00000000004016A1                 mov     eax, cs:dword_4AC054
.text:00000000004016A7                 test    eax, eax
.text:00000000004016A9                 jz      short loc_4016CC
.text:00000000004016AB                 lea     rcx, aWowYouFindIt ; "WoW,you find it\n"
.text:00000000004016B2                 call    sub_424D60
.text:00000000004016B7                 lea     rdx, unk_4AC030
.text:00000000004016BE                 lea     rcx, aNuaactfS  ; "NUAACTF{%s}"
.text:00000000004016C5                 call    sub_424D60
.text:00000000004016CA                 jmp     short loc_4016D8
.text:00000000004016CC ; ---------------------------------------------------------------------------
.text:00000000004016CC
.text:00000000004016CC loc_4016CC:                             ; CODE XREF: main+5E↑j
.text:00000000004016CC                                         ; main+68↑j
.text:00000000004016CC                 lea     rcx, aTryAgain  ; "try again"
00000A8D 000000000040168D: main+4C (Synchronized with Hex View-1)
```

```
IDA is analysing the input file...
You may start to explore the input file right now.
---------------------------------------------------------------------------------------
Python 3.9.7 (tags/v3.9.7:1016ef3, Aug 30 2021, 20:19:38) [MSC v.1929 64 bit (AMD64)]
IDAPython 64-bit v7.4.0 final (serial 0) (c) The IDAPython Team <idapython@googlegroups.com>
---------------------------------------------------------------------------------------
```

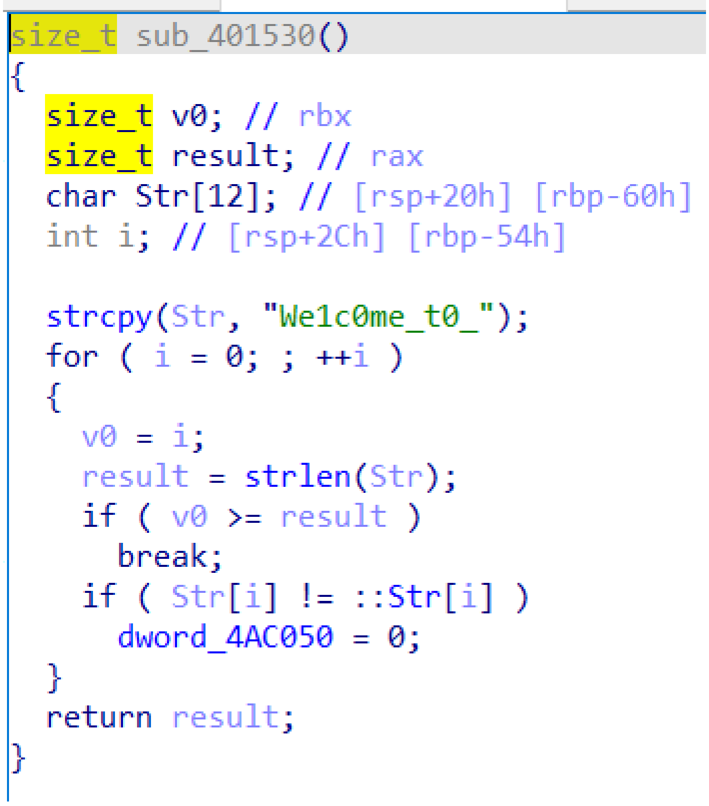
一开始进入汇编界面，于是按F5



```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  sub_40E8C0(argc, argv, envp);
  sub_424D60("Can you find where the flag is?\n");
  sub_424D60("Please input your flag:");
  sub_424D10("%s", Str);
  dword_4AC050 = 1;
  dword_4AC054 = 1;
  sub_401530();
  sub_4015A7();
  if ( dword_4AC050 && dword_4AC054 )
  {
    sub_424D60("WoW,you find it\n");
    sub_424D60("NUAACTF{%s}", Str);
  }
  else
  {
    sub_424D60("try again");
  }
  return 0;
}
```

发现如果是让 dword_4AC050 && dword_4AC054都为真，则str就是flag

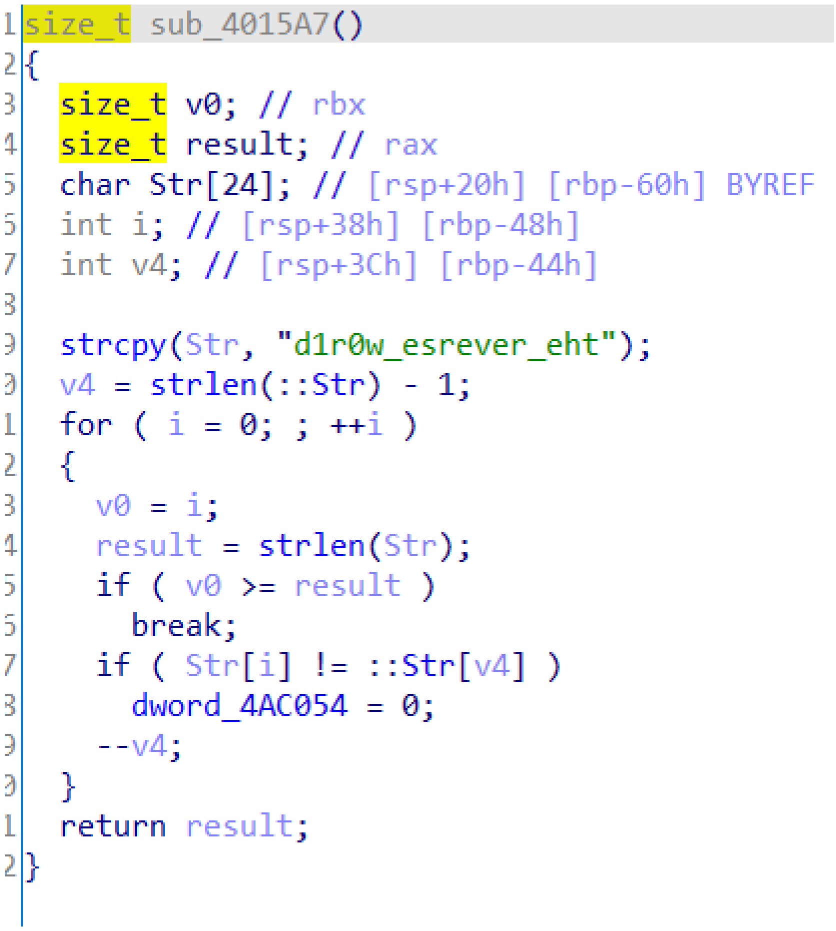
我们进入sub_401530和sub_4015A7观察函数，



```
size_t sub_401530()
{
  size_t v0; // rbx
  size_t result; // rax
  char Str[12]; // [rsp+20h] [rbp-60h]
  int i; // [rsp+2Ch] [rbp-54h]

  strcpy(Str, "We1c0me_t0_");
  for ( i = 0; ; ++i )
  {
    v0 = i;
    result = strlen(Str);
    if ( v0 >= result )
      break;
    if ( Str[i] != ::Str[i] )
      dword_4AC050 = 0;
  }
  return result;
}
```

第一个i=0，是正着来，



```
size_t sub_4015A7()
{
  size_t v0; // rbx
  size_t result; // rax
  char Str[24]; // [rsp+20h] [rbp-60h] BYREF
  int i; // [rsp+38h] [rbp-48h]
  int v4; // [rsp+3Ch] [rbp-44h]

  strcpy(Str, "d1r0w_esrever_eht");
  v4 = strlen(::Str) - 1;
  for ( i = 0; ; ++i )
  {
    v0 = i;
    result = strlen(Str);
    if ( v0 >= result )
      break;
    if ( Str[i] != ::Str[v4] )
      dword_4AC054 = 0;
    --v4;
  }
  return result;
}
```

第一个v4=str-1，发现是倒着来，

把str拼起来，答案即为NUAACTF{We1c0me_t0_the_reverse_w0r1d}