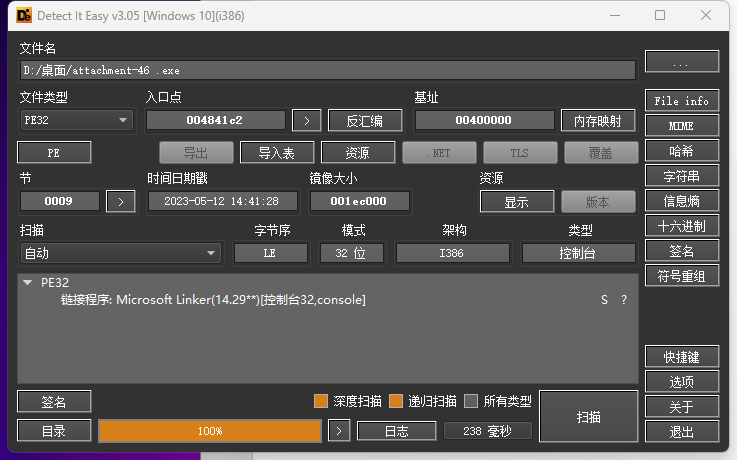
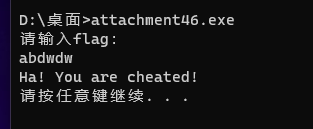
Die常规查壳

32位无壳PE文件

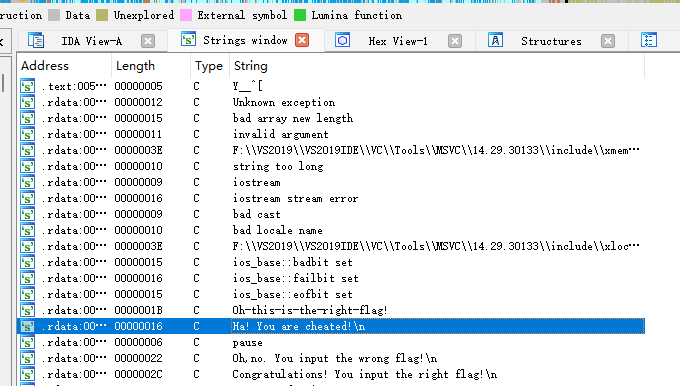


运行一下看看

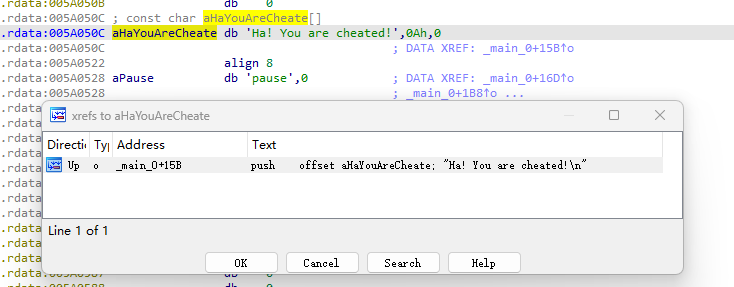


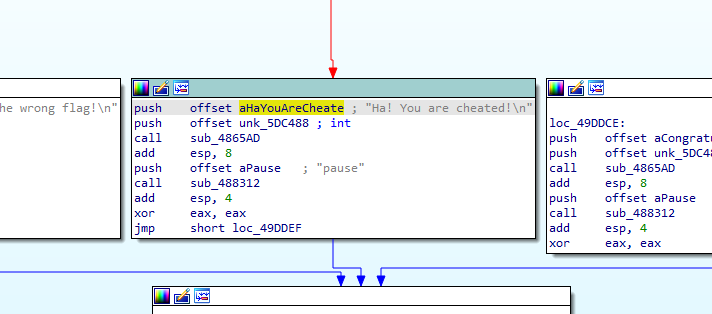
IDA打开

字符串列表找一下

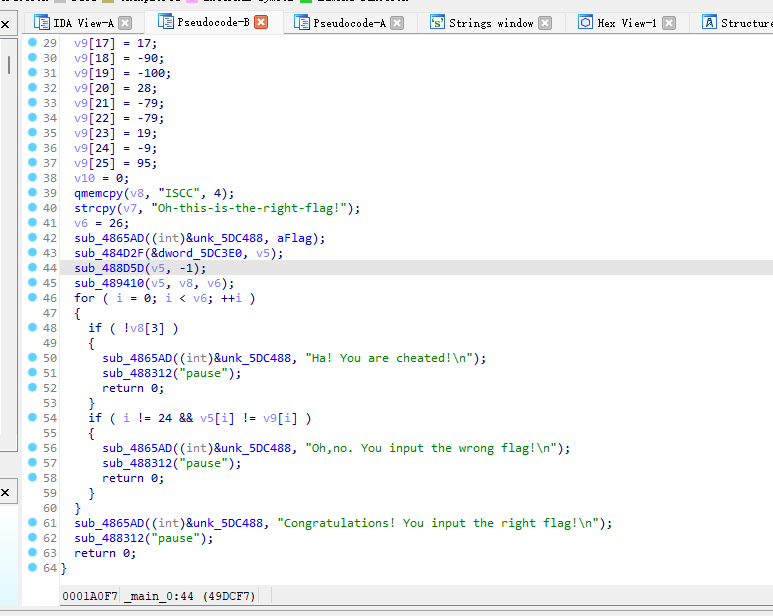


跟进一下这串字符





反编译查看main函数伪代码



简单分析一下

该程序的大致意思是用户输入字符串v5

经过加密后与数组v9进行比较

即v5为我们要得到的flag

那么将给出的v9数组进行解密就可以

编写解密脚本如下

v9 = [0 for i in range(26)]

v9[0] = 0xA5;

v9[1] = 67;

v9[2] = 83;

v9[3] = -108;

v9[4] = 96;

v9[5] = 84;

v9[6] = 77;

v9[7] = -68;

v9[8] = -20;

v9[9] = 90;

v9[10] = -84;

v9[11] = 107;

v9[12] = -127;

v9[13] = 122;

v9[14] = 70;

v9[15] = -67;

v9[16] = -93;

v9[17] = 95;

v9[18] = -89;

v9[19] = -68;

v9[20] = 76;

v9[21] = -95;

v9[22] = 80;

v9[23] = 112;

v9[24] = 0xF7;

v9[25] = ord('\_');

for i in range(25):

v9[i] = ((v9[i]&0xff) ^ 0x53)&0xff

for i in range(25-1):

v9[24-i] = v9[24-i] + v9[25-i]

for i in range(25):

v9 [i] = v9[i] + 30

c = ''

for i in range(25):

c += chr(v9[i]&0xff)

# print(c)

a = 'zabcdefghijklmnopqrstuvwxy'

a1 = 'abcdefghijklmnopqrstuvwxyz'

b = 'ZABCDEFGHIJKLMNOPQRSTUVWXY'

b1 = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'

f = 'H'+c[1:] + '}'

# f = 'HRBB{$DzI2{jlLf1mLXc3=4V!}'

p = ''

for m in f:

if m in a:

p+=a1[a.index(m)]

elif m in b:

p+=b1[b.index(m)]

else:

p+=m

print(p)