拖进ida进行分析，



首先是获取输入，然后中间的操作是将输入进行换位，放在v2地址处。

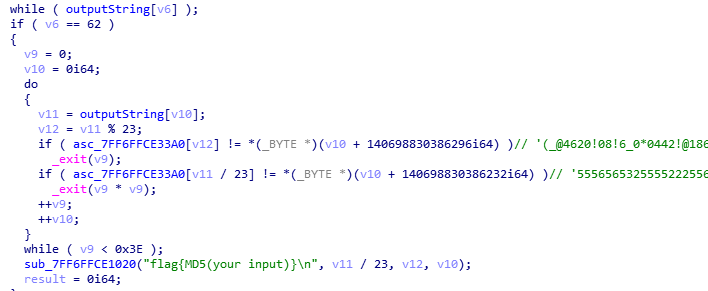
我们输入'1234567890abcdefghijklmnopqrstu'进行动态调试，可以得到v2是

'fg8hi94jk0lma52nobpqc6rsdtue731'，这样我们就就可以写脚本知道换位规则。

然后下面UnDecorateSymbolName函数，会根据v2得到outputString。



我们先看下面的流程得到outputString。



这就是根据outputString的62位字符进行简单的验证，我们写脚本爆破可以得到outputString。

str = '1234567890-=!@#$%^&\*()\_'  
str1 = '(\_@4620!08!6\_0\*0442!@186%%0@3=66!!974\*3234=&0^3&1@=&0908!6\_0\*&'  
str2 = '55565653255552225565565555243466334653663544426565555525555222'  
outputString = ""  
for i in range(62):  
 for j in range(1,127):  
 a = j % 23  
 b = j / 23  
 if(str[a] == str1[i]):  
 if(str[b] == str2[i]):  
 outputString += chr(j)  
print outputString

得到：private: char \* \_\_thiscall R0Pxx::My\_Aut0\_PWN(unsigned char \*)

然后看这篇文章<https://www.cnblogs.com/CodeMIRACLE/p/5343660.html>， 我们还原出v2为'?My\_Aut0\_PWN@R0Pxx@@AAEPADPAE@Z'。

然后我们再写脚本进行换位还原。

str1 = '1234567890abcdefghijklmnopqrstu'  
str2 = 'fg8hi94jk0lma52nobpqc6rsdtue731'  
str4 = '?My\_Aut0\_PWN@R0Pxx@@AAEPADPAE@Z'  
str = ""  
for i in range(len(str1)):  
 str += str4[str2.find(str1[i])]  
print str

得到 Z0@tRAEyuP@xAAA?M\_A0\_WNPx@@EPDP

