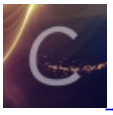
Kanxue看雪KCTF2019-Q1第六题【Repwn】Writeup

原创

iqiqiya 于 2019-03-26 21:16:26 发布 391 收藏
分类专栏： 我的逆向之路 我的CTF之路 ------看雪KCTF2019-Q1 我的CTF进阶之路 文章标签： Repwn KCTF2019-Q1

本文链接：https://blog.csdn.net/xiangshangbashaonian/article/details/88830451

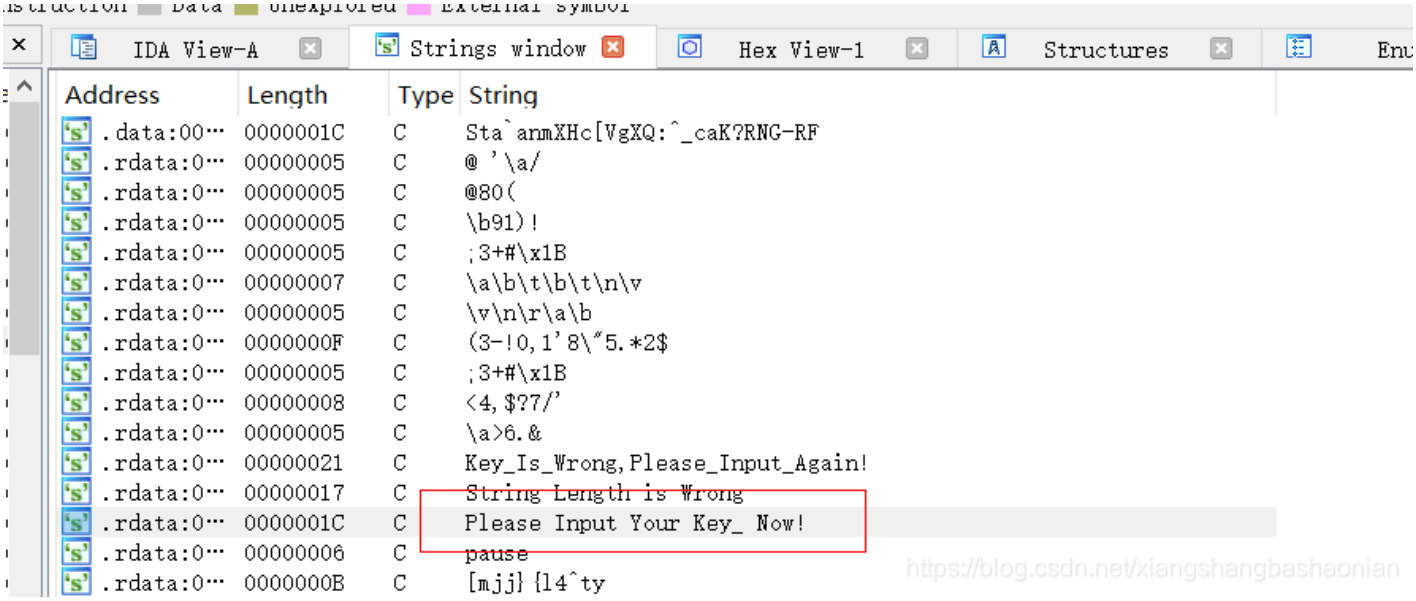

我的逆向之路 同时被 3 个专栏收录
108 篇文章 10 订阅
订阅专栏


我的CTF之路
92 篇文章 5 订阅
订阅专栏

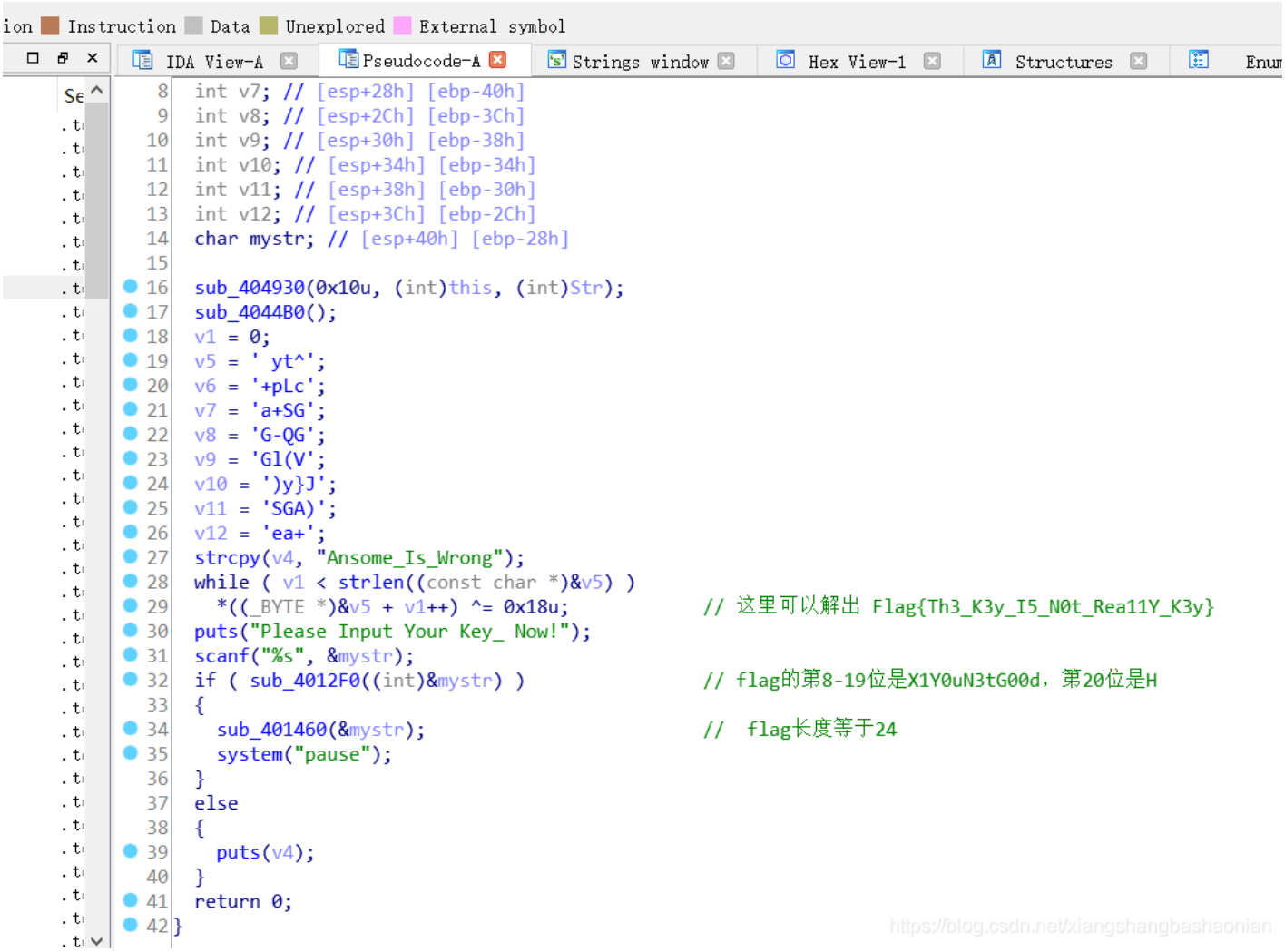

------看雪KCTF2019-Q1
4 篇文章 0 订阅
订阅专栏

> 第六题：Repwn

PEiD查壳，无壳 直接载入IDA shift+f12分析字符串



sub_4014C0()分析如下：

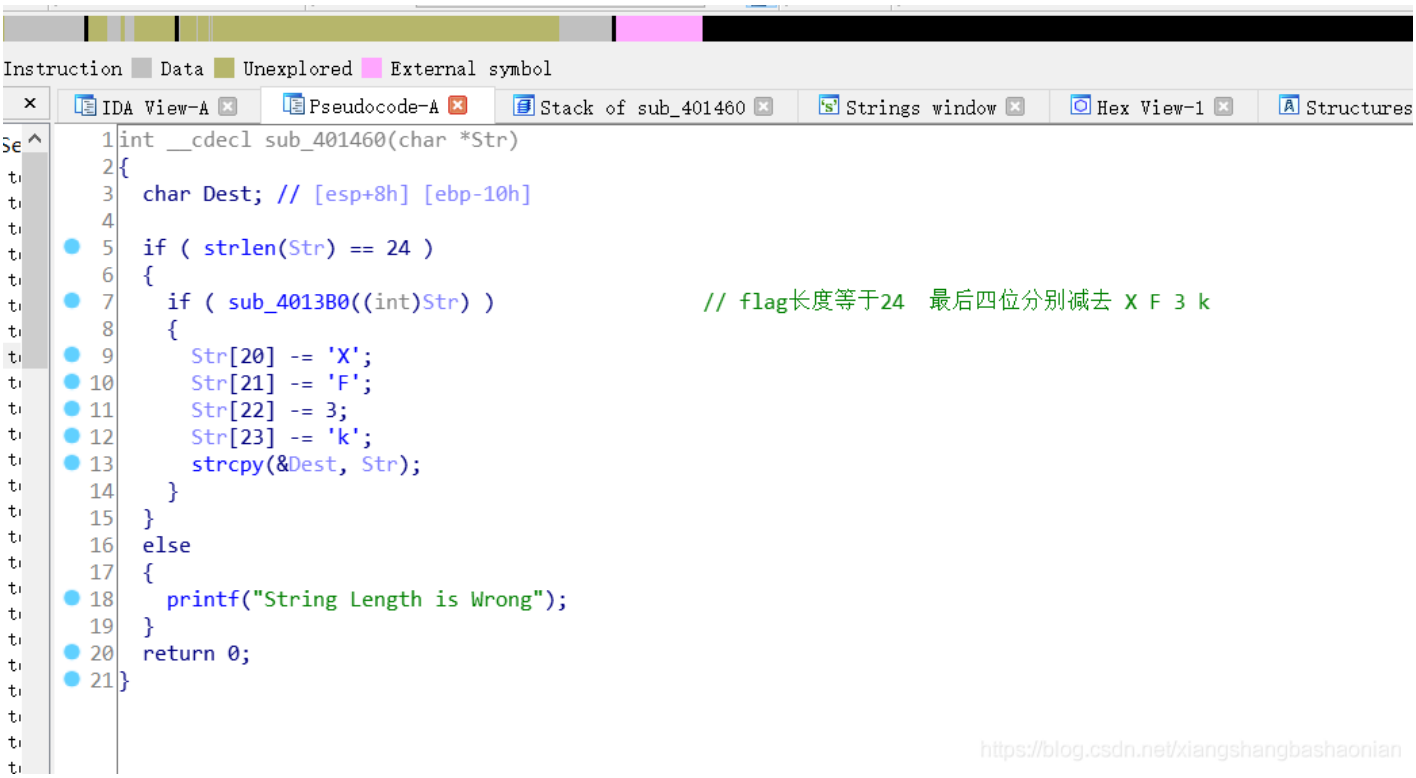


```
int v7; // [esp+28h] [ebp-40h]
int v8; // [esp+2Ch] [ebp-3Ch]
int v9; // [esp+30h] [ebp-38h]
int v10; // [esp+34h] [ebp-34h]
int v11; // [esp+38h] [ebp-30h]
int v12; // [esp+3Ch] [ebp-2Ch]
char mystr; // [esp+40h] [ebp-28h]

sub_404930(0x10u, (int)this, (int)Str);
sub_4044B0();
v1 = 0;
v5 = ' yt^';
v6 = '+pLc';
v7 = 'a+SG';
v8 = 'G-QG';
v9 = 'Gl(V';
v10 = ')y}J';
v11 = 'SGA)';
v12 = 'ea+';
strcpy(v4, "Ansome_Is_Wrong");
while ( v1 < strlen((const char *)&v5) )
  *((_BYTE *)&v5 + v1++) ^= 0x18u;            // 这里可以解出 Flag{Th3_K3y_I5_N0t_Rea11Y_K3y}
puts("Please Input Your Key_ Now!");
scanf("%s", &mystr);
if ( sub_4012F0((int)&mystr) )                // flag的第8-19位是X1Y0uN3tG00d，第20位是H
{
  sub_401460(&mystr);                         //  flag长度等于24
  system("pause");
}
else
{
  puts(v4);
}
return 0;
}
```


sub_4012F0()可以得到flag的第8-19位是X1Y0uN3tG00d，第20位是H

双击进入sub_401460()



```
int __cdecl sub_401460(char *Str)
{
  char Dest; // [esp+8h] [ebp-10h]

  if ( strlen(Str) == 24 )
  {
    if ( sub_4013B0((int)Str) )               // flag长度等于24  最后四位分别减去 X F 3 k
    {
      Str[20] -= 'X';
      Str[21] -= 'F';
      Str[22] -= 3;
      Str[23] -= 'k';
      strcpy(&Dest, Str);
    }
  }
  else
  {
    printf("String Length is Wrong");
  }
  return 0;
}
```


可以先分析sub_4013B0

```
signed int __cdecl sub_4013B0(int a1)
{
  int v1; // ebx
  int v2; // ecx
  int v3; // esi
  signed int result; // eax

  sub_401380(a1);
  v1 = dword_40802C + 1000 * dword_408020[0] + 100 * dword_408024 + 10 * dword_408028;
  v2 = dword_408034 + 10 * dword_408030;
  v3 = dword_40803C + 10 * dword_408038;
  if ( 2 * (v1 + v2) != 4040 || 3 * v2 / 2 + 100 * v3 != 115 )
    goto LABEL_2;
  result = 1;
  if ( v1 - 110 * v3 != 1900 )
  {
    printf("Key_Is_Wrong,Please_Input_Again!");
LABEL_2:
    result = 0;
  }
  return result;
}
```

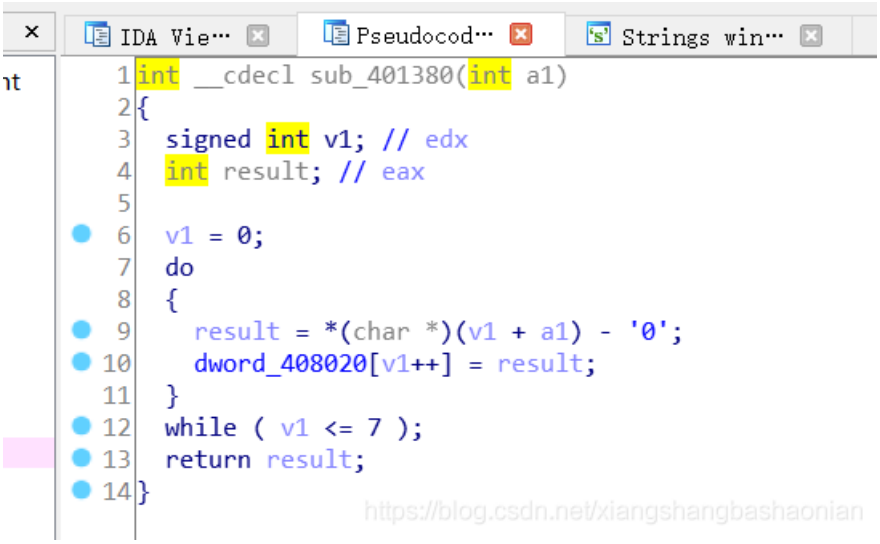

sub_4013B0取输入第一部分前8个字符按aaaabbcc转为整数, 校验是否满足方程组(aaaa + bb) * 2 == 4040 && (3 * bb / 2) + (100 * cc) == 115 && aaaa - 110 * cc == 1900

这里可以用z3求解

```
from z3 import *
aaaa = Int('aaaa')
bb = Int('bb')
cc = Int('cc')
s = Solver()
s.add(aaaa>0,aaaa<10000)
s.add(bb>0,bb<100)
s.add(cc>0,cc<100)
s.add((aaaa + bb) * 2 == 4040)
s.add((3 * bb / 2) + (100 * cc) == 115)
s.add(aaaa - 110 * cc == 1900)
m = s.model()
print(m[aaaa].as_long())
print(m[bb].as_long())
print(m[cc].as_long())
```

求得20101001

这里如果不明白 可以结合sub_401380()进行理解

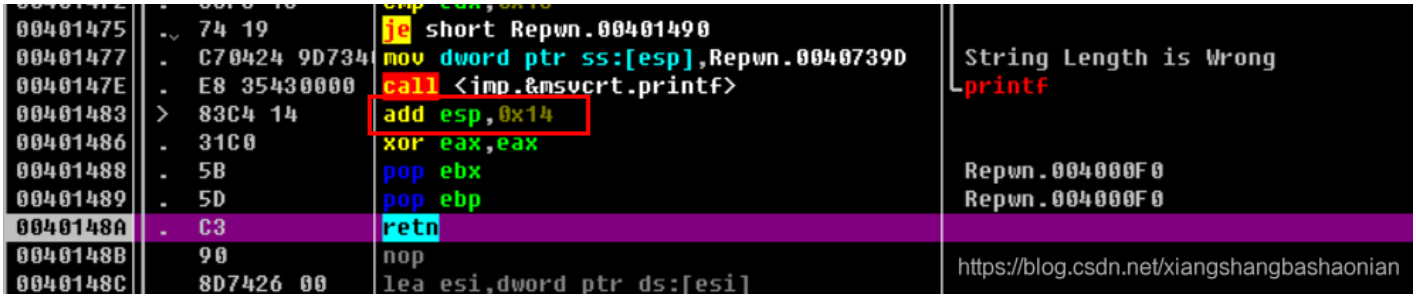


实现了atoi函数 将前8位 作为字符串转换为整型

所以可以用如下脚本：

```
for one in xrange(0,10):
    for two in xrange(0,10):
        for three in xrange(0,10):
            for four in xrange(0,10):
                for five in xrange(0,10):
                    for six in xrange(0,10):
                        for seven in xrange(0,10):
                            for eight in xrange(0,10):
                                v1 = 1000 * one + 100 * two + 10 * three + four
                                v2 = 10 * five + six
                                v3 = 10 * seven + eight
                                if v1 + v2 == 2020 and 100 * v3 + 3 * v2 / 2 == 115 and v1 - 110 * v3 == 19
                                    print one,two,three,four,five,six,seven,eight
#2 0 1 0 1 0 0 1
```

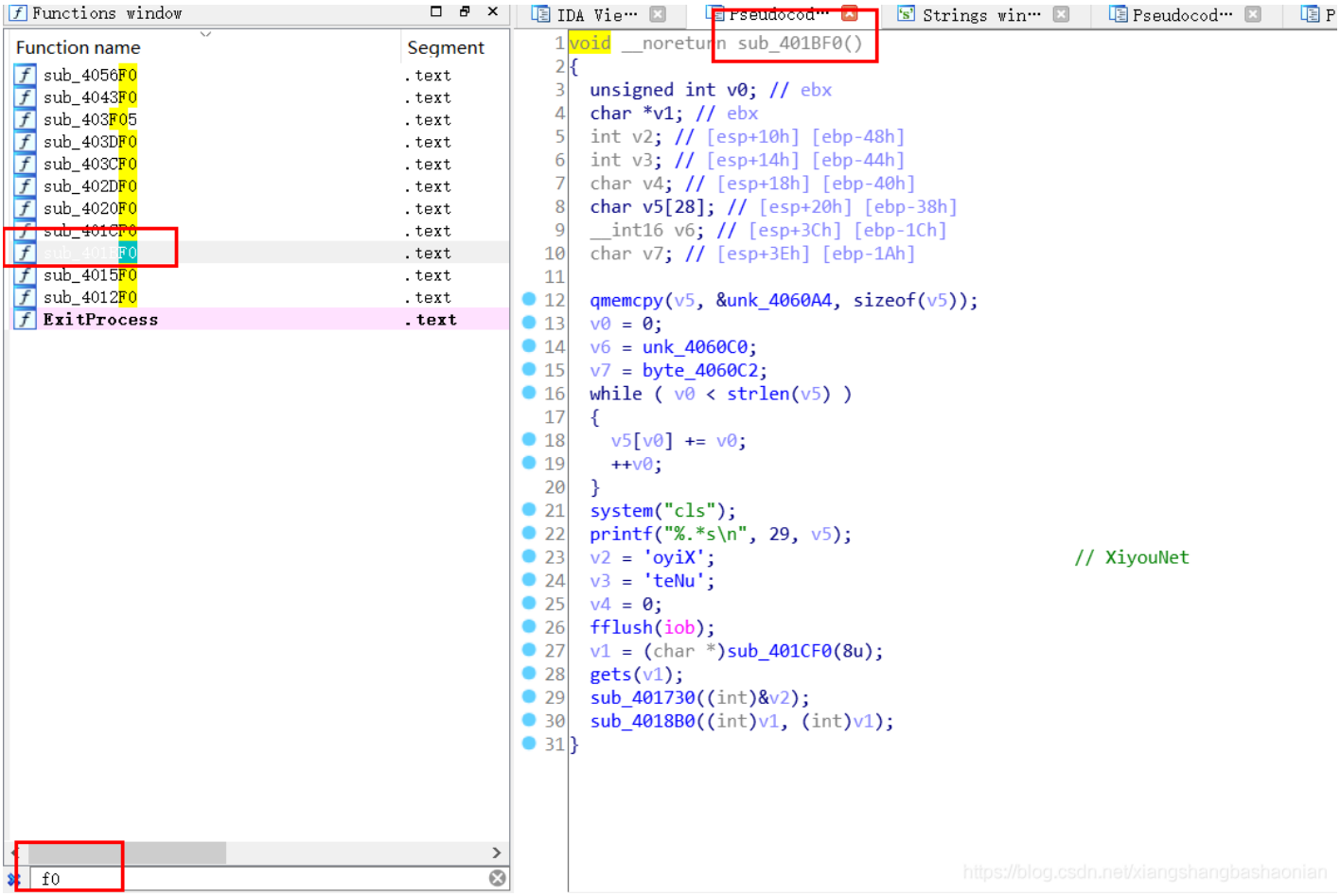
OD进行动态调试 输入20101001X1Y0uN3tG00dHF3k



局部变量buf长度为0x14，因此会造成栈溢出，恰好flag后四位会覆盖返回地址

由于flag[20]='H'，flag[20]-'X'=0xf0，考虑到小端序，所以只能选地址对齐0xf0的函数

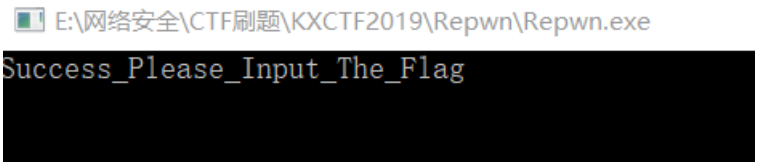
这里还可以根据查找字符串引用来确定



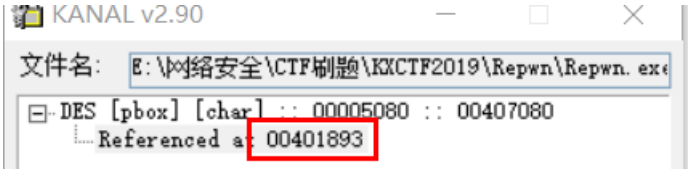
也可以用所有的进行验证　要注意字节溢出 高位舍去

```
  F0 1B 40 00
+ 58 46 03 6B
--------------
  48 61 43 6B
   H  a  C  k
```

得到20101001X1Y0uN3tG00dHaCk



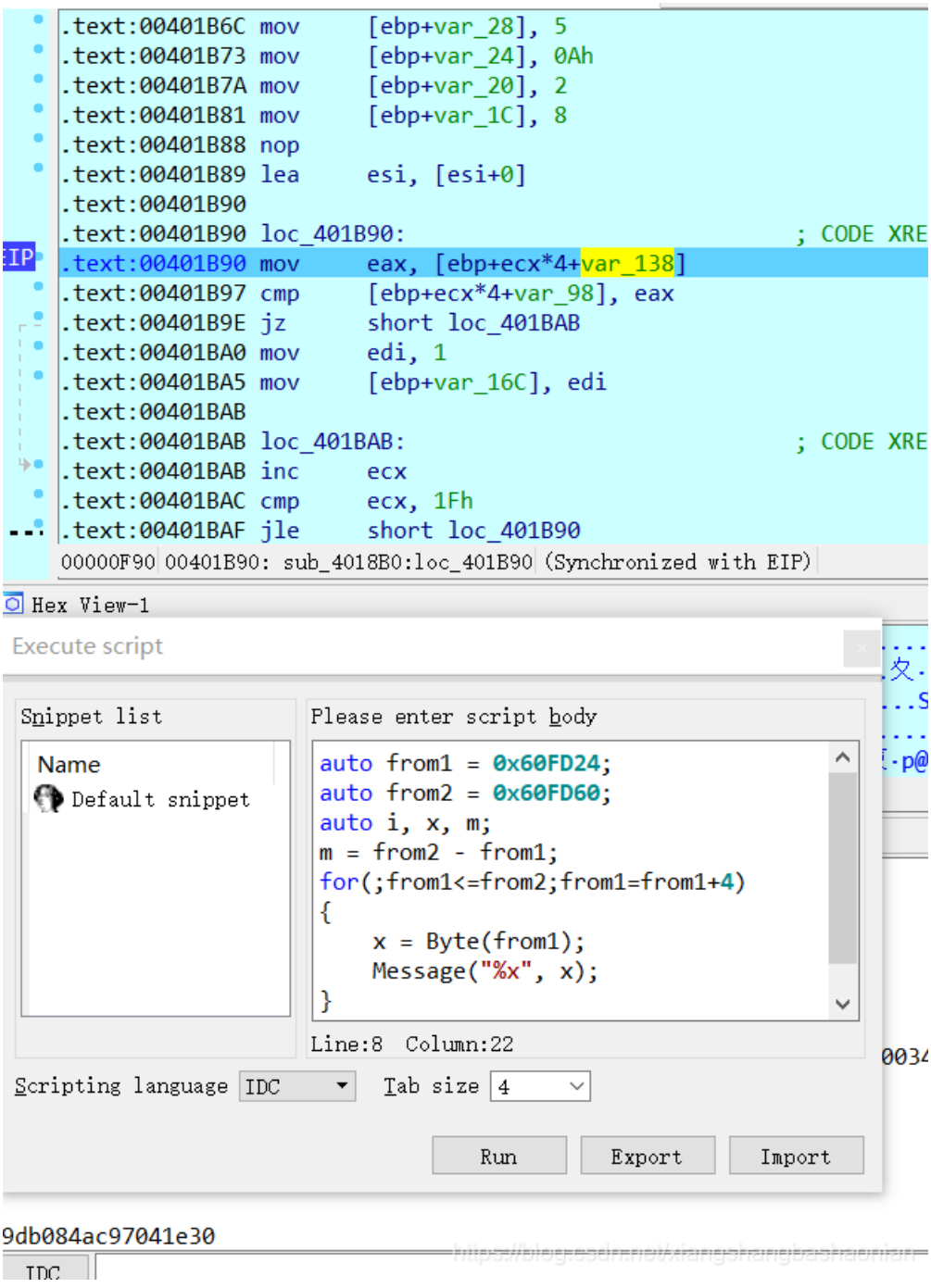
接着就是再次获取输入　sub_401730()与sub_4018b0()　将XiyouNet作为key值把我们的输入进行DES加密



最后与给定的密文进行比较 验证是否一致

```
110  v29 = 8;
111  while ( 1 )
112  {
113    if ( Dst[v8] != v12[v8] )
114      v9 = 1;
115    if ( ++v8 > 31 )
116    {
117      if ( !v9 )
118        printf(Format);
119      putchar(10);
120      system("pause");
121      ExitProcess(0);
122    }
123  }
124}
```


我们可以直接使用IDC脚本提取密文

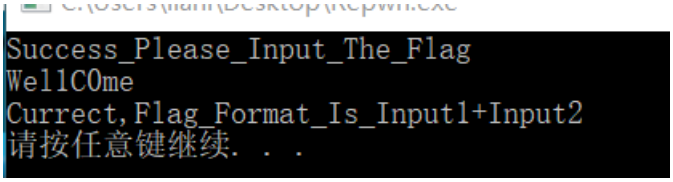


最后编写python脚本进行DES解密或者使用PYG密码学工具即可：

```
from Crypto.Cipher import DES
des = DES.new('XiyouNet')
s = '9db084ac97041e30'.decode('hex')
print(des.decrypt(s))
#Wel1C0me
```

最后的flag是input1+input2

也就是20101001X1Y0uN3tG00dHaCkWel1C0me



参考链接：

https://bbs.pediy.com/thread-250242.htm

https://bbs.pediy.com/thread-250229.htm