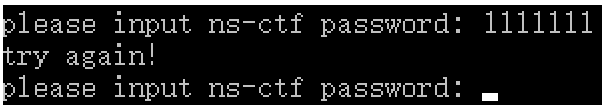
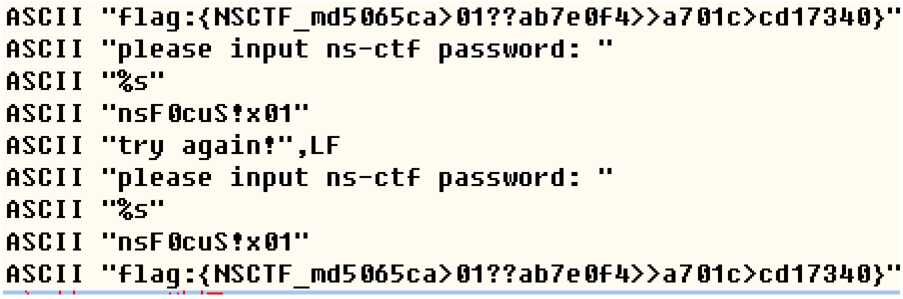
首先运行程序，程序提示输入密码，我们随便输入一组数据结果如下：



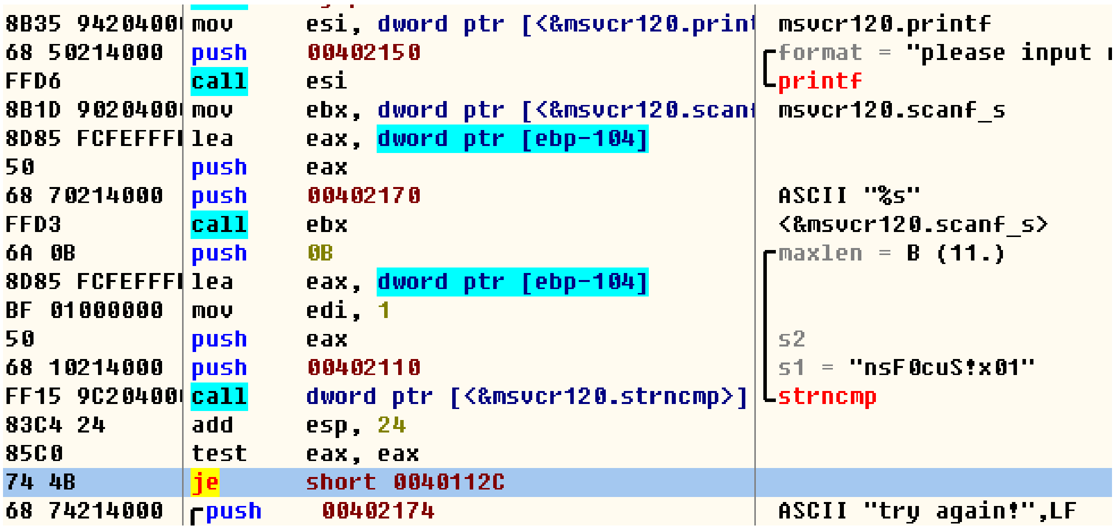
```
please input ns-ctf password: 1111111
try again!
please input ns-ctf password: _
```

可以看到程序给出错误提示，使用 OD 打开程序，查找->所有参考文本字串，结果如下



```
ASCII "flag:{NSCTF_md5065ca>01??ab7e0f4>>a701c>cd17340}"
ASCII "please input ns-ctf password: "
ASCII "%s"
ASCII "nsF0cuS!x01"
ASCII "try again!",LF
ASCII "please input ns-ctf password: "
ASCII "%s"
ASCII "nsF0cuS!x01"
ASCII "flag:{NSCTF_md5065ca>01??ab7e0f4>>a701c>cd17340}"
```

转到“try again!”所在位置，



```
8B35 9420400 mov     esi, dword ptr [<&msvcr120.print  msvcr120.printf
68 50214000  push    00402150                         ┌format = "please input 
FFD6         call    esi                              └printf
8B1D 9020400 mov     ebx, dword ptr [<&msvcr120.scan  msvcr120.scanf_s
8D85 FCFEFFF lea     eax, dword ptr [ebp-104]
50           push    eax
68 70214000  push    00402170                          ASCII "%s"
FFD3         call    ebx                               <&msvcr120.scanf_s>
6A 0B        push    0B                               ┌maxlen = B (11.)
8D85 FCFEFFF lea     eax, dword ptr [ebp-104]         │
BF 01000000  mov     edi, 1                           │
50           push    eax                              │s2
68 10214000  push    00402110                         │s1 = "nsF0cuS!x01"
FF15 9C20400 call    dword ptr [<&msvcr120.strncmp>]  └strncmp
83C4 24      add     esp, 24
85C0         test    eax, eax
74 4B        je      short 0040112C
68 74214000  ┌push    00402174                         ASCII "try again!",LF
```

这就很明显了，程序首先读取我们的输入，然后和内存中的字符串比较，相等则注册成功，不等则注册失败。而且可以很清楚的看到内存中的字符串为“nsF0cuS!x01”，即为所求。