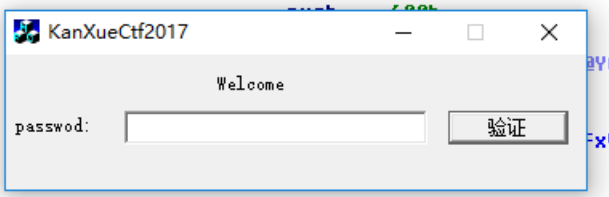
看雪hello

转载

weixin_30611509 于 2019-03-22 13:23:00 发布 128 收藏
原文链接：http://www.cnblogs.com/chuxinbubian/p/10577654.html

在看雪做了一道题目很简单，但是还是记录一下自己的学习。

```
46                      ; [00000029 BYTES: COLLAPSED FUNCTION AfxInitialize
6F                      ; ---------------------------------------------------
6F E9 00 00 00 00               jmp     $+5
74                      ; ---------------------------------------------------
74
74                      loc_402074:                             ; CODE XREF
74 68 00 06 00 00               push    600h
79 6A 00
7B E8 C6 FF FF FF
80 A2 18 41 40 00
85 C3
86
8C CC CC CC CC
90
90                      ; =============== S U B R O U T I N E ===============
90
90
90                      sub_402090      proc near               ; DATA XREF
90 8D 4D 84                     lea     ecx, [ebp-7Ch]
93 E8 48 F1 FF FF               call    sub_4011E0
98 C3                           retn
98                      sub_402090      endp
```



用ida打开，然后shift+F12查看

Address	Length	Type	String
.rdata:00403554	0000000C	C	关于(&A)...
.rdata:00403560	00000006	C	pass!
.rdata:00403568	00000006	C	恭喜!
.rdata:00403570	00000006	C	加油!
.rdata:00403578	00000006	C	错了!
.rdata:00403580	00000017	C	WelcomeToKanXueCtf2(
.rdata:00403598	0000000C	C	请输入pass!
.rdata:0040392C	0000000A	C	MFC42.DLL
.rdata:00403976	0000000B	C	MSVCRT.dll
.rdata:00403A8A	0000000D	C	KERNEL32.dll
.rdata:00403B2C	0000000B	C	USER32.dll

这里可以看到基本的结构，转到pass查看

```
.rdata:00403540 00 15 40 00                             dd offset sub_401500
.rdata:00403544 40 1D 40 00                             dd offset ?OnSetFont@CDialog@@UAEXPAVCFont@@@Z ; CDialog::OnSetFont(CF
.rdata:00403548 F0 17 40 00                             dd offset sub_4017F0
.rdata:0040354C 34 1D 40 00                             dd offset ?OnCancel@CDialog@@MAEXXZ ; CDialog::OnCancel(void)
.rdata:00403550 2E 1D 40 00                             dd offset ?PreInitDialog@CDialog@@MAEXXZ ; CDialog::PreInitDialog(void
.rdata:00403554                         ; char NewItem[]
.rdata:00403554 B9 D8 D3 DA 28 26 41 29+NewItem         db '关于(&A)...',0      ; DATA XREF: sub_401500+72↑o
.rdata:00403560                         ; char Text[]
.rdata:00403560 70 61 73 73 21 00       Text            db 'pass!',0            ; DATA XREF: sub_401770+10↑o
.rdata:00403566 00 00                                   align 4
.rdata:00403568                         ; char Caption[]
.rdata:00403568 B9 A7 CF B2 21 00       Caption         db '恭喜!',0            ; DATA XREF: sub_401770+B↑o
.rdata:0040356E 00 00                                   align 10h
.rdata:00403570                         ; char asc_403570[]
.rdata:00403570 BC D3 D3 CD 21 00       asc_403570      db '加油!',0            ; DATA XREF: sub_4017B0+10↑o
.rdata:00403576 00 00                                   align 4
.rdata:00403578                         ; char aA[]
.rdata:00403578 B4 ED C1 CB 21 00       aA              db '错了!',0            ; DATA XREF: sub_4017B0+B↑o
.rdata:0040357E 00 00                                   align 10h
.rdata:00403580                         ; char Str2[]
.rdata:00403580 57 65 6C 63 6F 6D 65 54+Str2            db 'WelcomeToKanXueCtf2017',0
.rdata:00403580 6F 4B 61 6E 58 75 65 43+                                        ; DATA XREF: sub_4017F0:loc_401854↑o
.rdata:00403597 00                                      align 4
.rdata:00403598 C7 EB CA E4 C8 EB 70 61+aIFIpass        db '请输入pass!',0      ; DATA XREF: sub_4017F0+55↑o
.rdata:004035A4 00 00 00 00                             align 8
.rdata:004035A8 FF FF FF FF DA 1F 40 00+stru_4035A8     _SCOPETABLE_ENTRY <0FFFFFFFFh, offset loc_401FDA, offset loc_401FEE>
.rdata:004035A8 EE 1F 40 00                                                     ; DATA XREF: start+5↑o
.rdata:004035A8                                                                 ; SEH scope table for function 401E9C
.rdata:004035B4 00 00 00 00                             align 8
.rdata:004035B8 20 05 93 19 01 00 00 00+stru_4035B8     dd 19930520h            ; Magic
.rdata:004035B8 D8 35 40 00 00 00 00 00+                                        ; DATA XREF: SEH_401150↑o
.rdata:004035B8 00 00 00 00 00 00 00 00+                dd 1                    ; Count
.rdata:004035B8 00 00 00 00 00 00 00 00+                dd offset stru_4035B8.Info; InfoPtr
```

发现ATA XREF: sub_401770+Bo打开这里

```
        ; Attributes: bp-based frame

        sub_401770      proc near               ; CODE XREF: sub_4017F0+79↓p

        hProcess        = dword ptr -4

                        push    ebp
                        mov     ebp, esp
                        sub     esp, 44h
                        push    ebx
                        push    esi
                        push    edi
                        push    0               ; uType
0                       push    offset Caption  ; "恭喜!"
0                       push    offset Text     ; "pass!"
                        push    0               ; hWnd
0 00                    call    ds:MessageBoxA
0 00                    call    ds:GetCurrentProcess
                        mov     [ebp+hProcess], eax
                        push    0               ; uExitCode
                        mov     eax, [ebp+hProcess]
                        push    eax             ; hProcess
0 00                    call    ds:TerminateProcess
                        pop     edi
                        pop     esi
                        pop     ebx
                        mov     esp, ebp
```

```
.text:00401845 68 98 35 40 00                  push    offset aIFIpass ; "请输入pass!"
.text:0040184A 8B 4D FC                        mov     ecx, [ebp+var_4]
.text:0040184D E8 C0 05 00 00                  call    ?MessageBoxA@CWnd@@QAEHPBD0I@Z ; CWnd::MessageBoxA(char const *,char const *
.text:00401852 EB 21                           jmp     short loc_401875
.text:00401854                         ; ---------------------------------------------------------------------------
.text:00401854
.text:00401854                         loc_401854:                             ; CODE XREF: sub_4017F0+4F↑j
.text:00401854 68 80 35 40 00                  push    offset Str2     ; "WelcomeToKanXueCtf2017"
.text:00401859 8B 55 F8                        mov     edx, [ebp+Str1]
.text:0040185C 52                              push    edx             ; Str1
.text:0040185D E8 2E 06 00 00                  call    strcmp
.text:00401862 83 C4 08                        add     esp, 8
.text:00401865 85 C0                           test    eax, eax
.text:00401867 75 07                           jnz     short loc_401870
.text:00401869 E8 02 FF FF FF                  call    sub_401770
.text:0040186E EB 05                           jmp     short loc_401875
.text:00401870                         ; ---------------------------------------------------------------------------
.text:00401870
.text:00401870                         loc_401870:                             ; CODE XREF: sub_4017F0+77↑j
.text:00401870 E8 3B FF FF FF                  call    sub_4017B0
.text:00401875
.text:00401875                         loc_401875:                             ; CODE XREF: sub_4017F0+62↑j
.text:00401875                                                                 ; sub_4017F0+7E↑j
.text:00401875 5F                              pop     edi
.text:00401876 5E                              pop     esi
.text:00401877 5B                              pop     ebx
```

flag就是WelcomeToKanXueCtf2017

转载于:https://www.cnblogs.com/chuxinbubian/p/10577654.html