实验一 PE文件破解和插桩注入

1.自编helloworld程序，解释汇编代码，写上注释。

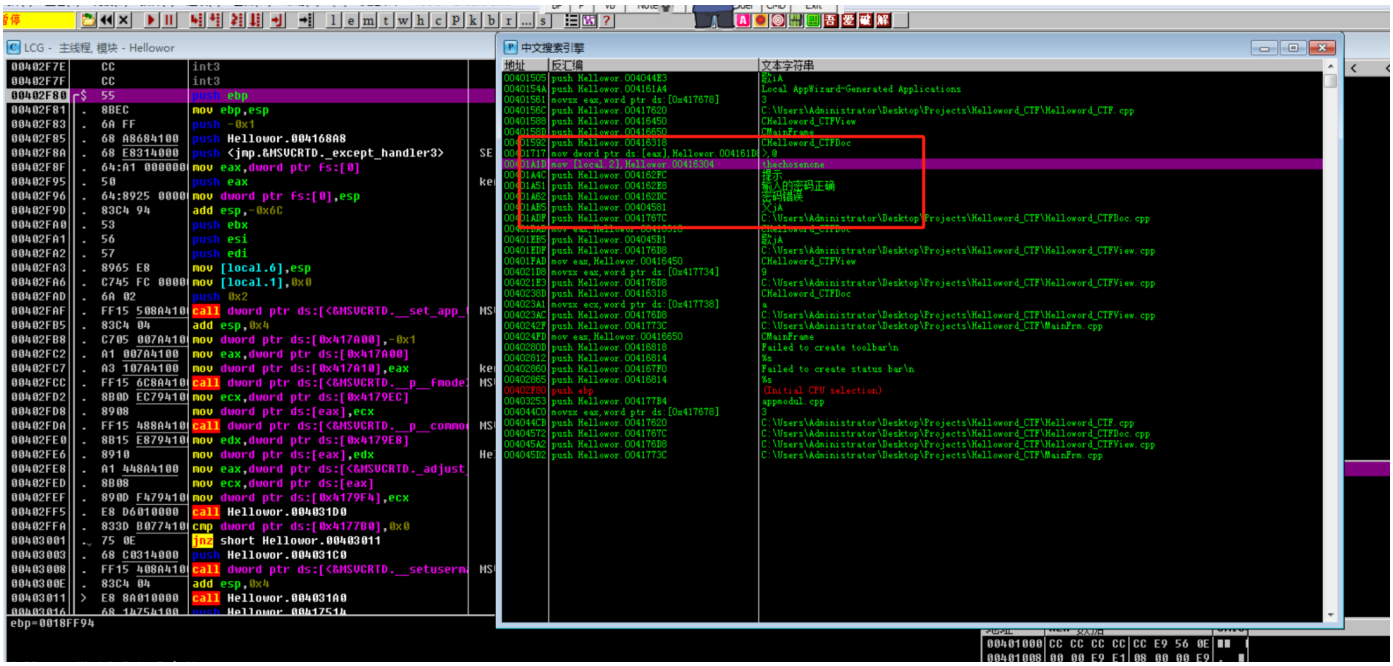
```
push ebp
mov ebp,esp
#这两行代码保存了当前的栈帧指针（ebp）并设置一个新的栈帧指针。
6A FF |push -0x1
#这一行将一个值 -0x1 推送到栈上。
68 38014200 |push demo.00420138
68 243E4000 |push demo.__except_handler3ldBlock?9?$DO>; SE 处理程序安装
#这两行将两个函数地址推送到栈上。第一个地址是 demo.00420138，第二个地址是 demo.__except_handler3ldBlo
64:A1 0000000|mov eax,dword ptr fs:[0]
#这一行将FS段寄存器的值（通常用于线程局部存储）的偏移为0的地址处的值加载到eax寄存器中。
50 |push eax; kernel32.BaseThreadInitThunk
64:8925 00000|mov dword ptr fs:[0],esp
#这两行代码保存了当前的线程环境，包括堆栈指针，以备后续的异常处理。
83C4 F0 |add esp,-0x10
#这一行减小了栈指针，为局部变量分配了16个字节的空间。
53 |push ebx
56 |push esi
57 |push edi
#这三行将寄存器ebx、esi和edi的值推送到堆栈上，以保存这些寄存器的值。
8965 E8 |mov [local.6],esp
#这一行将当前堆栈指针的值保存到局部变量local.6中。
FF15 3C514200|call dword ptr ds:[<&KERNEL32.GetVersion>]; kernel32.GetVersion
#这一行调用了kernel32.GetVersion函数
A3 E4354200 |mov dword ptr ds:[_osvermSetgerLister],eax; kernel32.BaseThreadInitThunk
A1 E4354200 |mov eax,dword ptr ds:[_osvermSetgerLister]
C1E8 08 |shr eax,0x8
25 FF000000 |and eax,0xFF
A3 F0354200 |mov dword ptr ds:[_winminorabCounter_Installed],eax; kernel32.BaseThreadInitThunk
#这些指令用于获取操作系统的主版本号和次版本号，并保存到相关的全局变量中
8B0D E4354200|mov ecx,dword ptr ds:[_osvermSetgerLister]
81E1 FF000000|and ecx,0xFF
890D EC354200|mov dword ptr ds:[_winmajorlocrpDefer],ecx
8B15 EC354200|mov edx,dword ptr ds:[_winmajorlocrpDefer]
C1E2 08 |shl edx,0x8
0315 F0354200|add edx,dword ptr ds:[_winminorabCounter_Installed]
```

```
8915 E8354200|mov dword ptr ds:[_winverwnVece],edx ; demo.<ModuleEntryPoint>
#这些指令用于获取操作系统的次次版本号和构建号，并保存到相关的全局变量中。
A1 E4354200 |mov eax,dword ptr ds:[_osvermSetgerLister]
C1E8 10 |shr eax,0x10
25 FFFF0000 |and eax,0xFFFF
A3 E4354200 |mov dword ptr ds:[_osvermSetgerLister],eax
#这些指令用于获取操作系统的构建号，并保存到相关的全局变量中。
6A 00 |push 0x0
E8 9D2A0000 |call demo._heap_initgClientooksSinceed
#这两行代码用于初始化堆内存管理，并调用demo._heap_initgClientooksSinceed函数。
83C4 04 |add esp,0x4
85C0 |test eax,eax; kernel32.BaseThreadInitThunk
#这两行用于检查堆内存管理的初始化是否成功。它们对eax寄存器中的值进行测试，以查看是否为零。
75 0A |jnz short demo.004011B4
6A 1C |push 0x1C
E8 CF000000 |call demo.fast_error_exitoldstdstalled
83C4 04 |add esp,0x4
#如果初始化失败（test指令的结果非零），则跳转到demo.004011B4，否则继续执行。在这种情况下，它将调用demo.
C745 FC 00000|mov [local.1],0x0
#这一行将值0x0 存储到局部变量local.1 中。
E8 10270000 |call demo._ioiniterify_blockObjectsled
#这一行调用了demo._ioiniterify_blockObjectsled函数。
```

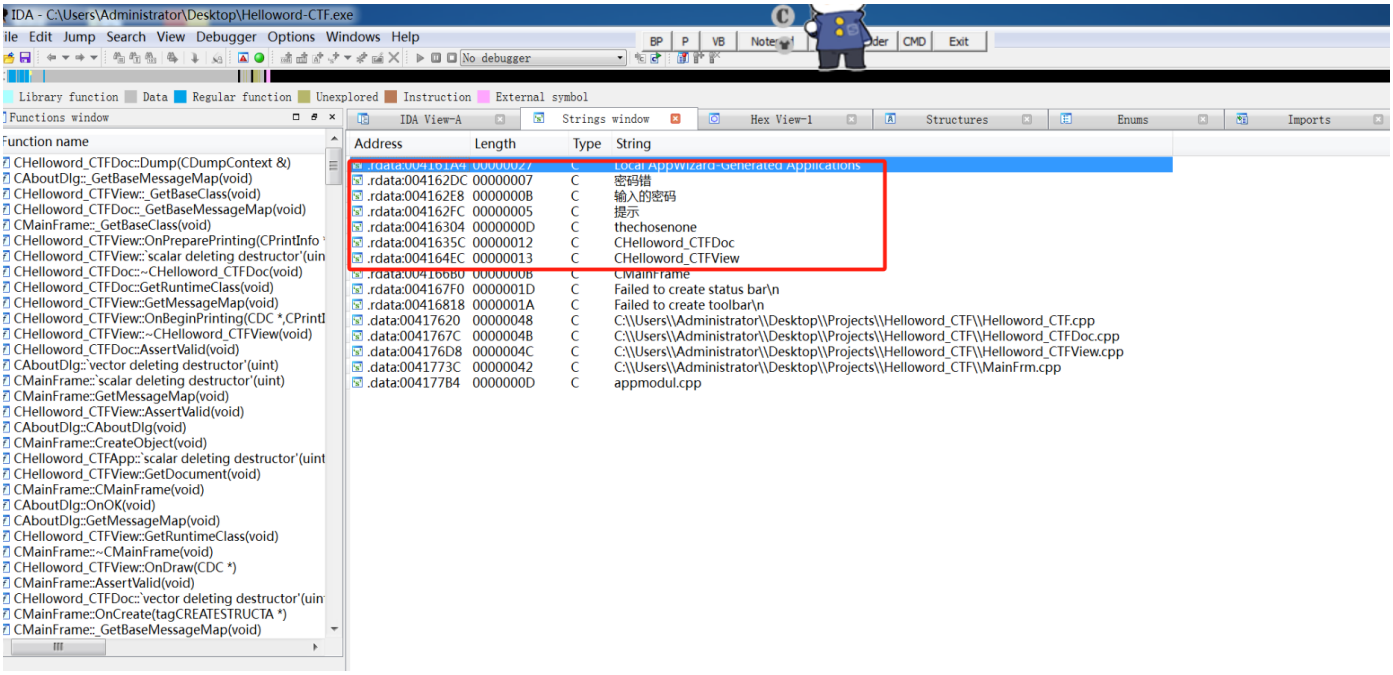
2.对Helloworld_CTF.exe进行逆向分析

(1) 找密码

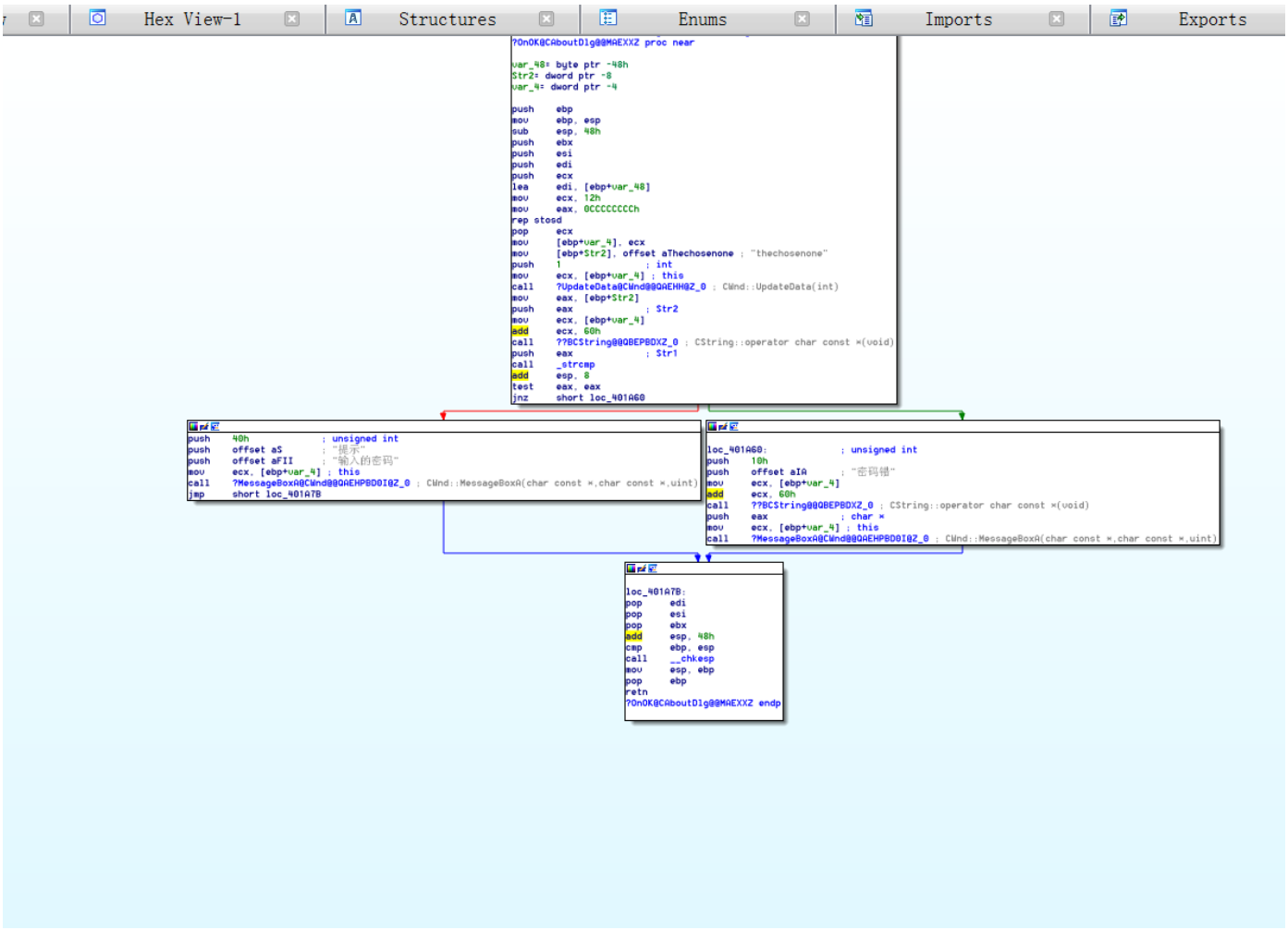
- 目标：找到Helloworld_CTF.exe程序的正确密码并验证
- 过程记录：
- onlydebug 对文件进行分析，使用**中文搜索引擎**找到判断密码是否正确的位置：



- 在 IDA 中打开程序，再通过 搜索字符串 得到下表，判断 `thechosenone` 很可能是密码：



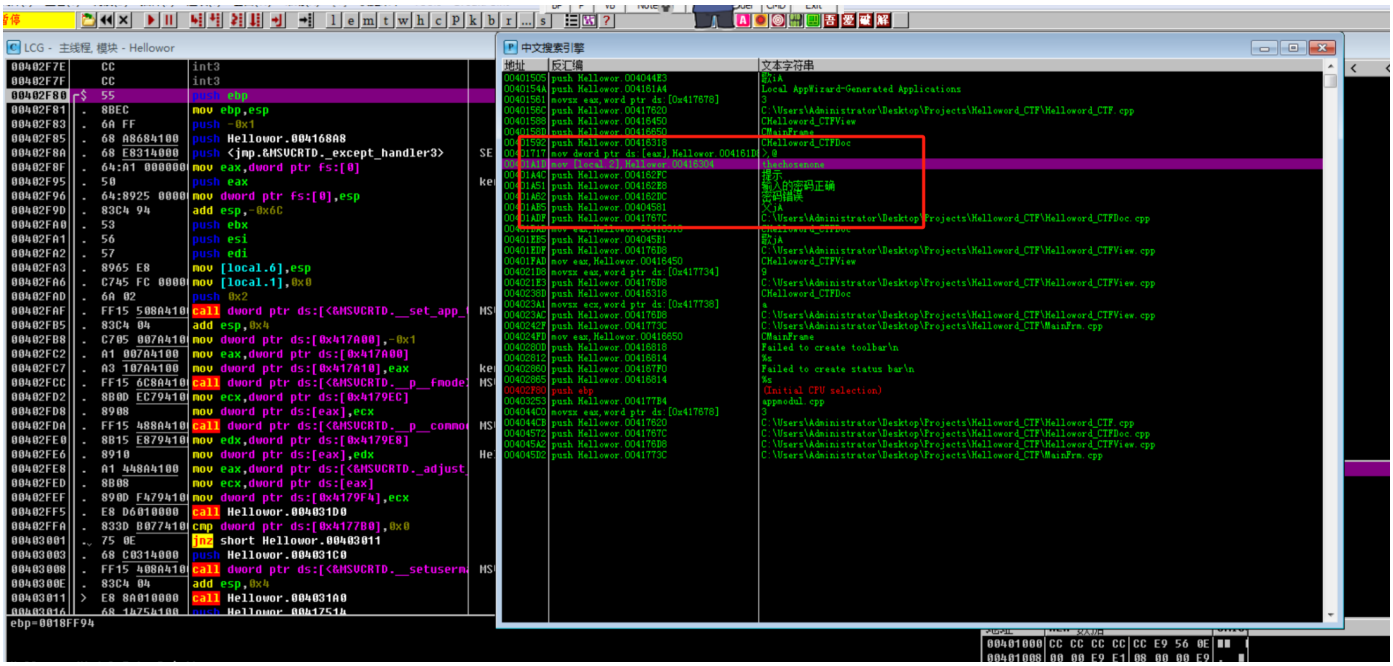
- 点击 `thechosenone` 字符串，可跳转到至下列详解图（IDA View），在空白处右键，操作后跳转至代码模,空白处右键后点击 `Graph view` 转换至图形模式（或直接空格跳转）,可得该程序的关系图：

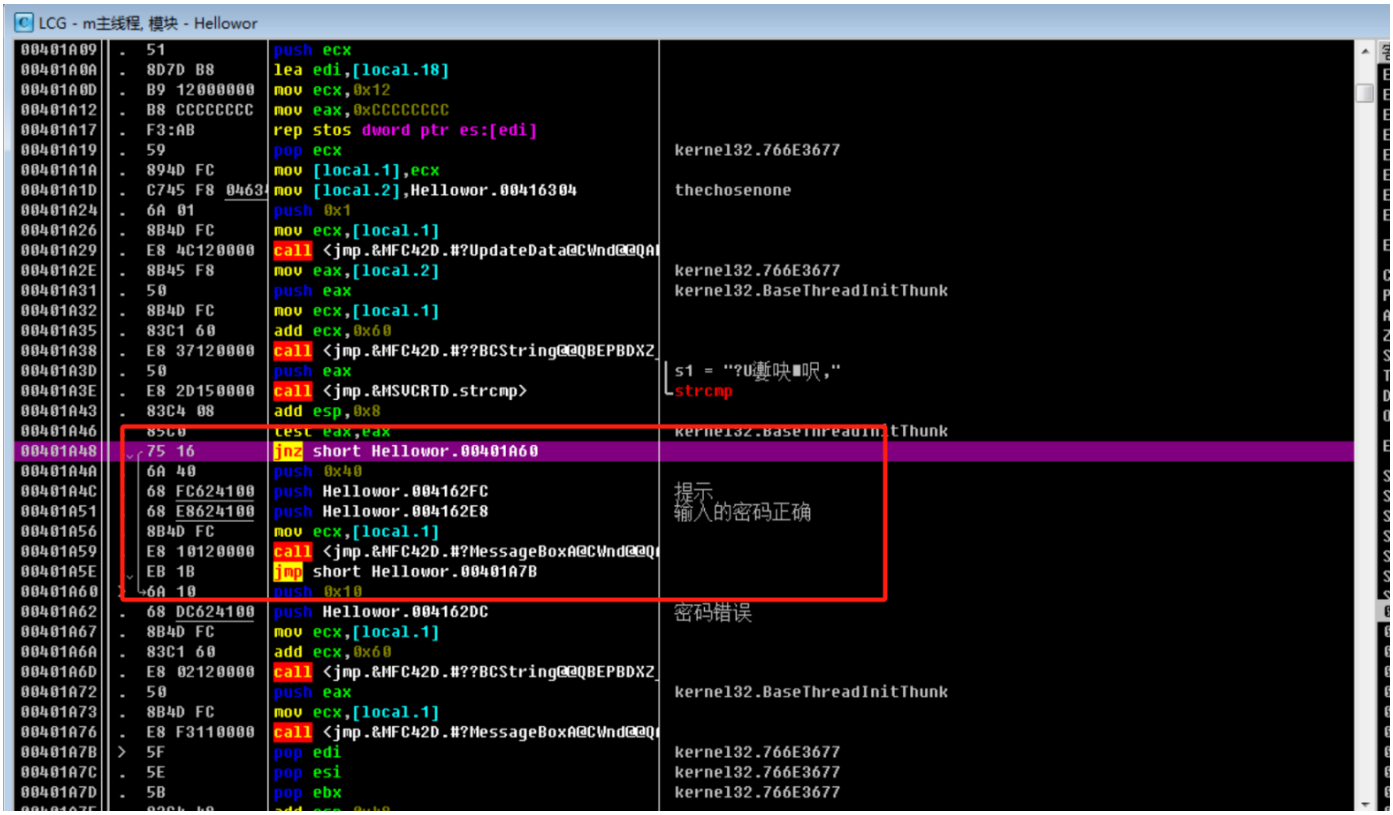


- 可以分析得出，该程序就是通过比对输入的密码和该字符串是否一致来判断对错，所以 thechosenone 就是密码。

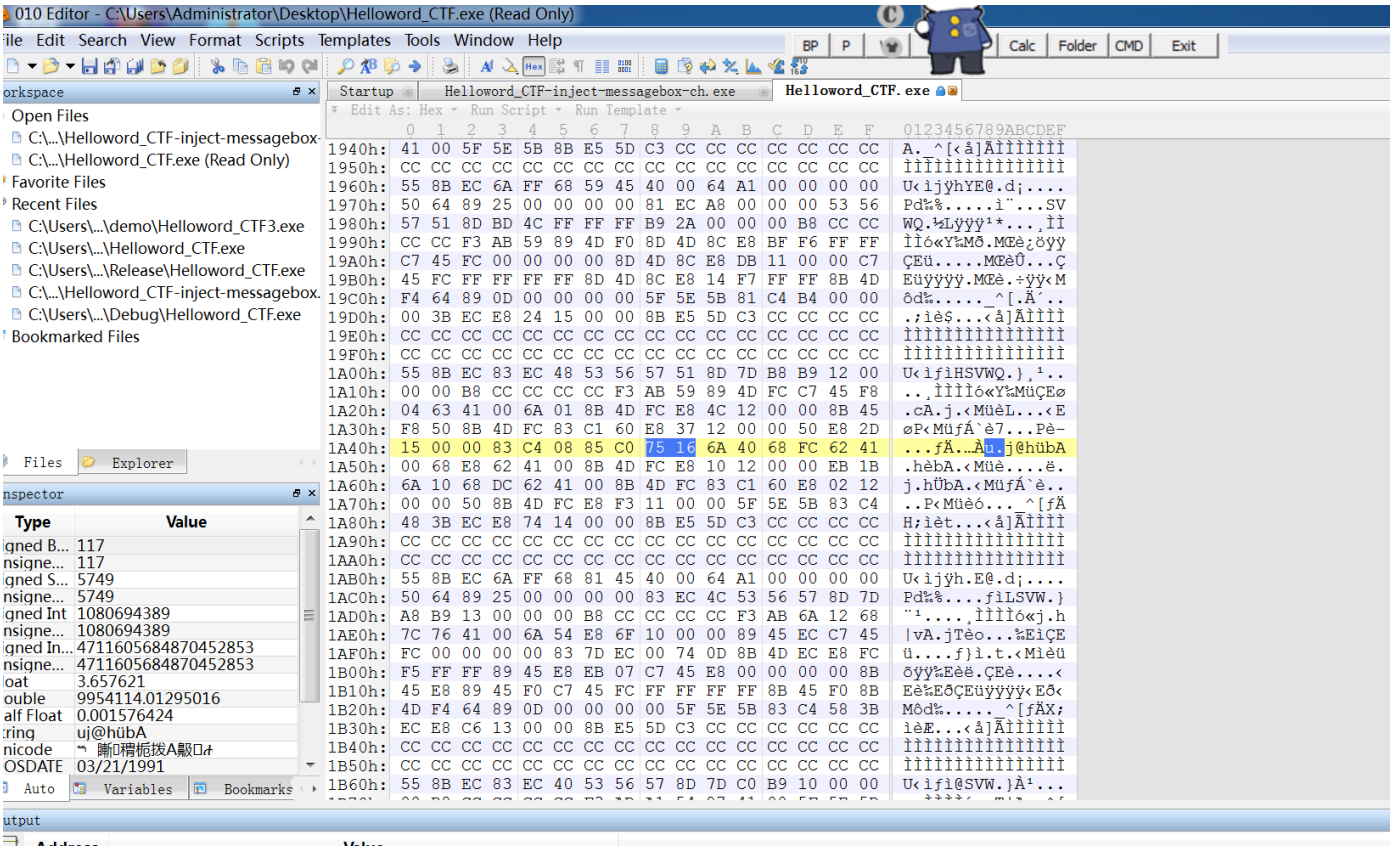
(2)改逻辑

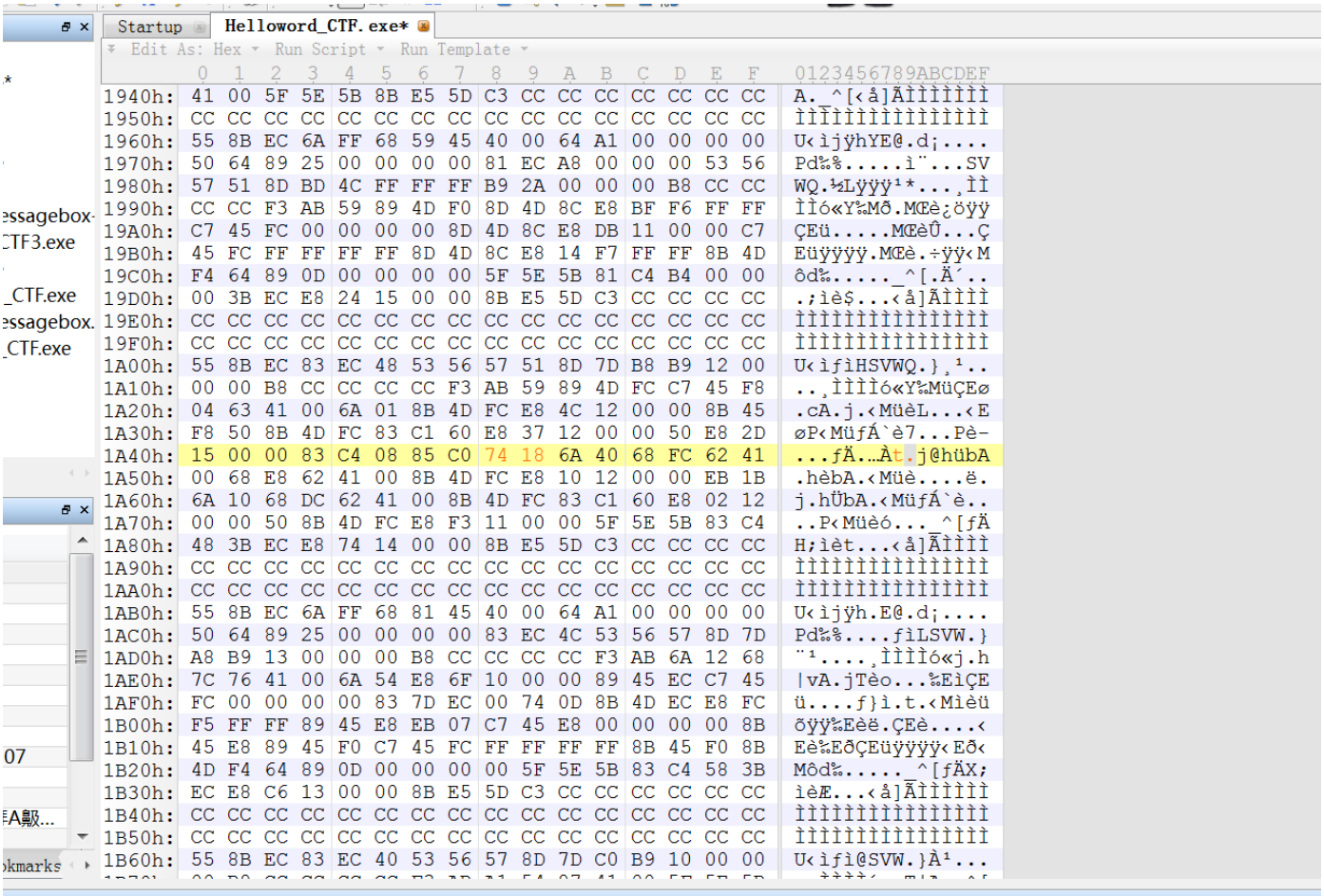
- 目标：是 输入错误的密码 时，会弹出 密码正确 的弹窗， 输入正确的密码 时，反而会提示 密码错误 。
- onlydebug 对文件进行分析，使用**中文搜索引擎**找到判断密码是否正确的位置,再找到判断密码是否正确的汇编代码的位置：



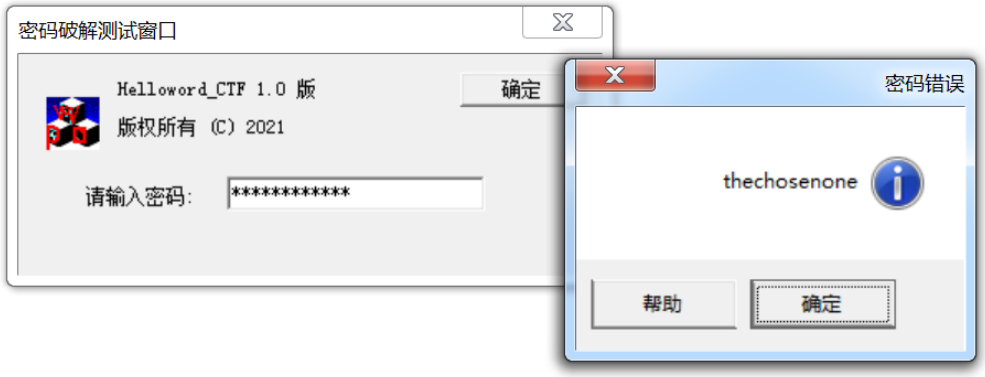


- 使用 010editor 打开文件，得到二进制形式的文件，通过 ollyDebug 中对应的汇编代码在文件中存储位置（即最左侧一栏的十六进制地址），或者直接使用 ctrl F 搜索 7516 ,将其改为 7418 （记得先将文件属性里的只读模式取消）：


010 Editor - C:\Users\Administrator\Desktop\Helloword_CTF.exe (Read Only)
File Edit Search View Format Scripts Templates Tools Window Help
Workspace
Open Files
Favorite Files
Recent Files
Bookmarked Files
Startup
Helloword_CTF-inject-messagebox-ch.exe
Helloword_CTF.exe
Edit As: Hex
Run Script
Run Template
Inspector
Type
Value
Files
Explorer
Auto
Variables
Bookmarks
Output


Startup
Helloword_CTF.exe*
Edit As: Hex
Run Script
Run Template

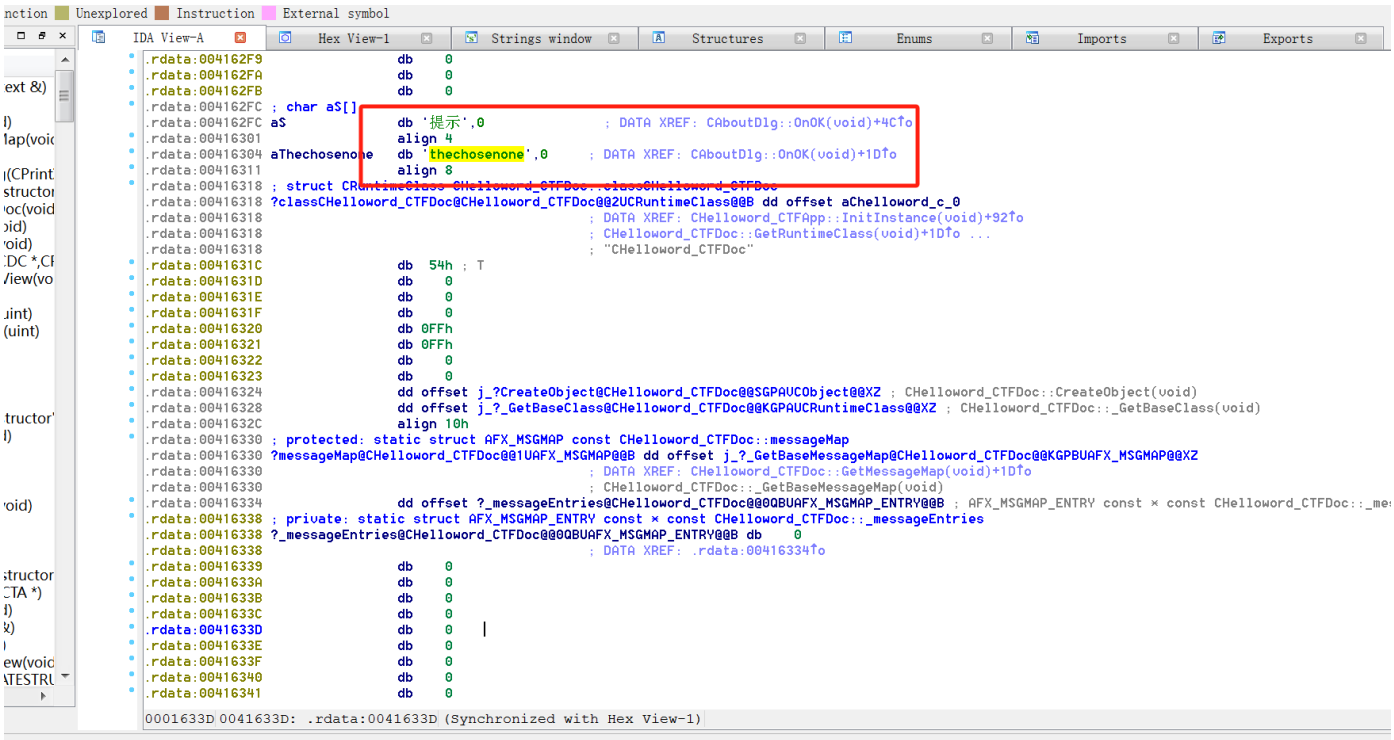
- 当输入正确密码时：

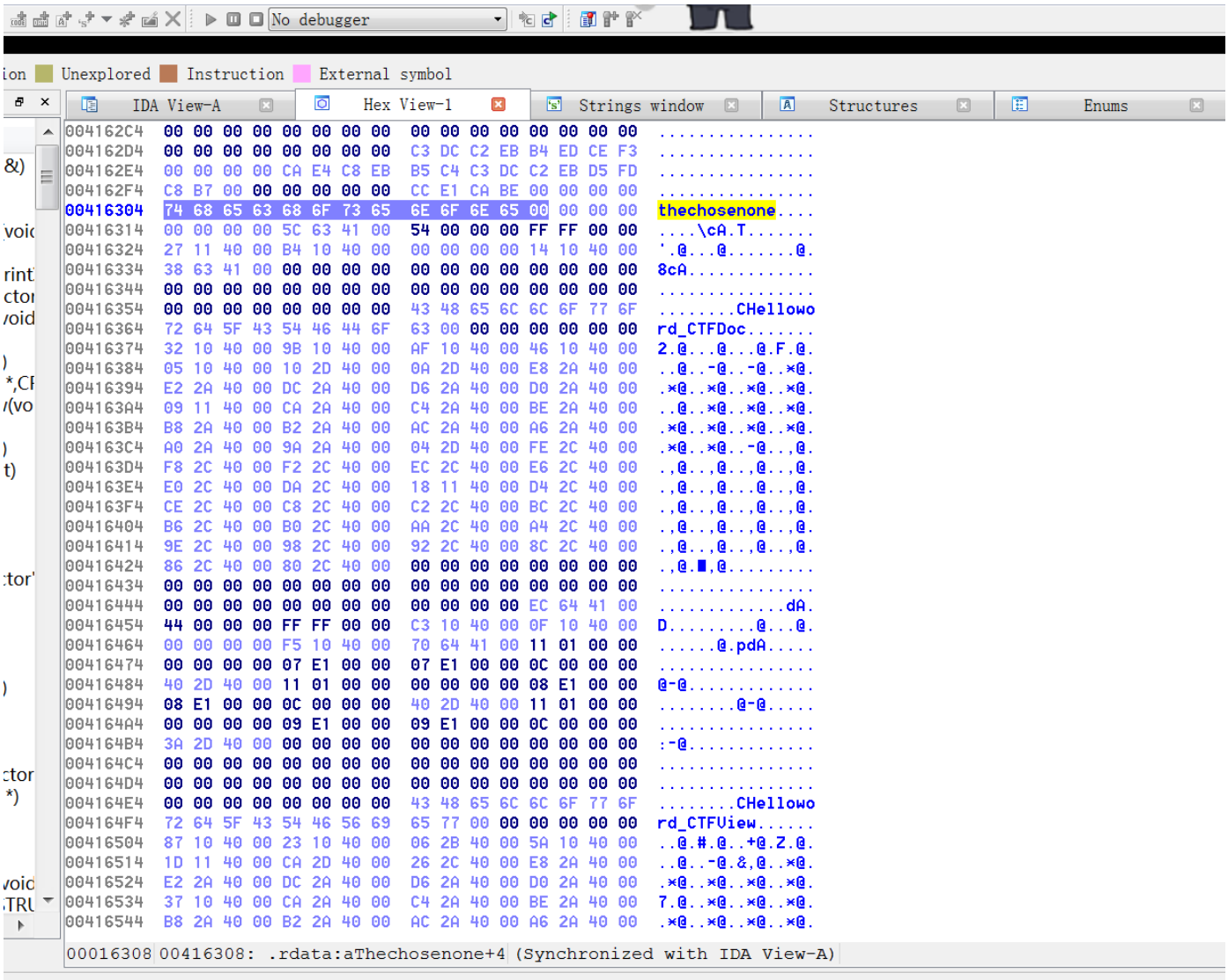


- 当输入错误密码时:

(3)改密码

- 通过 找密码 的过程，可以确认密码在文件中的存储位置:


nction Unexplored Instruction External symbol
IDA View-A
Hex View-1
Strings window
Structures
Enums
Imports
Exports
.rdata:004162F9 db 0
.rdata:004162FA db 0
.rdata:004162FB db 0
.rdata:004162FC ; char a$[]
.rdata:004162FC a$ db '提示',0 ; DATA XREF: CAboutDlg::OnOK(void)+4C↑o
.rdata:00416301 align 4
.rdata:00416304 aThechosenone db 'thechosenone',0 ; DATA XREF: CAboutDlg::OnOK(void)+1D↑o
.rdata:00416311 align 8
.rdata:00416318 ; struct CRuntimeClass CHelloword_CTFDoc::classCHelloword_CTFDoc
.rdata:00416318 ?classCHelloword_CTFDoc@CHelloword_CTFDoc@@2UCRuntimeClass@@B dd offset aCHelloword_c_0
.rdata:00416318 ; DATA XREF: CHelloword_CTFApp::InitInstance(void)+92↑o
.rdata:00416318 ; CHelloword_CTFDoc::GetRuntimeClass(void)+1D↑o ...
.rdata:00416318 ; "CHelloword_CTFDoc"
.rdata:0041631C db 54h ; T
.rdata:0041631D db 0
.rdata:0041631E db 0
.rdata:0041631F db 0
.rdata:00416320 db 0FFh
.rdata:00416321 db 0FFh
.rdata:00416322 db 0
.rdata:00416323 db 0
.rdata:00416324 dd offset j_?CreateObject@CHelloword_CTFDoc@@SGPAUCObject@@XZ ; CHelloword_CTFDoc::CreateObject(void)
.rdata:00416328 dd offset j_?_GetBaseClass@CHelloword_CTFDoc@@KGPAUCRuntimeClass@@XZ ; CHelloword_CTFDoc::_GetBaseClass(void)
.rdata:0041632C align 10h
.rdata:00416330 ; protected: static struct AFX_MSGMAP const CHelloword_CTFDoc::messageMap
.rdata:00416330 ?messageMap@CHelloword_CTFDoc@@1UAFX_MSGMAP@@B dd offset j_?_GetBaseMessageMap@CHelloword_CTFDoc@@KGPBUAFX_MSGMAP@@XZ
.rdata:00416330 ; DATA XREF: CHelloword_CTFDoc::GetMessageMap(void)+1D↑o
.rdata:00416330 ; CHelloword_CTFDoc::_GetBaseMessageMap(void)
.rdata:00416334 dd offset ?_messageEntries@CHelloword_CTFDoc@@0QBUAFX_MSGMAP_ENTRY@@B ; AFX_MSGMAP_ENTRY const × const CHelloword_CTFDoc::_me
.rdata:00416338 ; private: static struct AFX_MSGMAP_ENTRY const × const CHelloword_CTFDoc::_messageEntries
.rdata:00416338 ?_messageEntries@CHelloword_CTFDoc@@0QBUAFX_MSGMAP_ENTRY@@B db 0
.rdata:00416338 ; DATA XREF: .rdata:00416334↑o
.rdata:00416339 db 0
.rdata:0041633A db 0
.rdata:0041633B db 0
.rdata:0041633C db 0
.rdata:0041633D db 0
.rdata:0041633E db 0
.rdata:0041633F db 0
.rdata:00416340 db 0
.rdata:00416341 db 0
0001633D 0041633D: .rdata:0041633D (Synchronized with Hex View-1)


No debugger
ion Unexplored Instruction External symbol
IDA View-A
Hex View-1
Strings window
Structures
Enums
004162C4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
004162D4 00 00 00 00 00 00 00 00 C3 DC C2 EB B4 ED CE F3 ....
004162E4 00 00 00 00 CA E4 C8 EB B5 C4 C3 DC C2 EB D5 FD ....
004162F4 C8 B7 00 00 00 00 00 00 CC E1 CA BE 00 00 00 00 ....
00416304 74 68 65 63 68 6F 73 65 6E 6F 6E 65 00 00 00 00 thechosenone....
00416314 00 00 00 00 5C 63 41 00 54 00 00 00 FF FF 00 00 ....\cA.T.......
00416324 27 11 40 00 B4 10 40 00 00 00 00 00 14 10 40 00 '.@...@.......@.
00416334 38 63 41 00 00 00 00 00 00 00 00 00 00 00 00 00 8cA.............
00416344 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00416354 00 00 00 00 00 00 00 00 43 48 65 6C 6C 6F 77 6F ....CHellowo
00416364 72 64 5F 43 54 46 44 6F 63 00 00 00 00 00 00 00 rd_CTFDoc.......
00416374 32 10 40 00 9B 10 40 00 AF 10 40 00 46 10 40 00 2.@...@...@.F.@.
00416384 05 10 40 00 10 2D 40 00 0A 2D 40 00 E8 2A 40 00 ..@..-@..-@..*@.
00416394 E2 2A 40 00 DC 2A 40 00 D6 2A 40 00 D0 2A 40 00 .*@..*@..*@..*@.
004163A4 09 11 40 00 CA 2A 40 00 C4 2A 40 00 BE 2A 40 00 ..@..*@..*@..*@.
004163B4 B8 2A 40 00 B2 2A 40 00 AC 2A 40 00 A6 2A 40 00 .*@..*@..*@..*@.
004163C4 A0 2A 40 00 9A 2A 40 00 04 2D 40 00 FE 2C 40 00 .*@..*@..-@..,@.
004163D4 F8 2C 40 00 F2 2C 40 00 EC 2C 40 00 E6 2C 40 00 .,@..,@..,@..,@.
004163E4 E0 2C 40 00 DA 2C 40 00 18 11 40 00 D4 2C 40 00 .,@..,@...@..,@.
004163F4 CE 2C 40 00 C8 2C 40 00 C2 2C 40 00 BC 2C 40 00 .,@..,@..,@..,@.
00416404 B6 2C 40 00 B0 2C 40 00 AA 2C 40 00 A4 2C 40 00 .,@..,@..,@..,@.
00416414 9E 2C 40 00 98 2C 40 00 92 2C 40 00 8C 2C 40 00 .,@..,@..,@..,@.
00416424 86 2C 40 00 80 2C 40 00 00 00 00 00 00 00 00 00 .,@.■,@.........
00416434 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00416444 00 00 00 00 00 00 00 00 00 00 00 00 EC 64 41 00 ....dA.
00416454 44 00 00 00 FF FF 00 00 C3 10 40 00 0F 10 40 00 D.........@...@.
00416464 00 00 00 00 F5 10 40 00 70 64 41 00 11 01 00 00 ......@.pdA.....
00416474 00 00 00 00 07 E1 00 00 07 E1 00 00 0C 00 00 00 ....
00416484 40 2D 40 00 11 01 00 00 00 00 00 00 08 E1 00 00 @-@.............
00416494 08 E1 00 00 0C 00 00 00 40 2D 40 00 11 01 00 00 ....@-@.....
004164A4 00 00 00 00 09 E1 00 00 09 E1 00 00 0C 00 00 00 ....
004164B4 3A 2D 40 00 00 00 00 00 00 00 00 00 00 00 00 00 :-@.............
004164C4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
004164D4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
004164E4 00 00 00 00 00 00 00 00 43 48 65 6C 6C 6F 77 6F ....CHellowo
004164F4 72 64 5F 43 54 46 56 69 65 77 00 00 00 00 00 00 rd_CTFView......
00416504 87 10 40 00 23 10 40 00 06 2B 40 00 5A 10 40 00 ..@.#.@..+@.Z.@.
00416514 1D 11 40 00 CA 2D 40 00 26 2C 40 00 E8 2A 40 00 ..@..-@.&,@..*@.
00416524 E2 2A 40 00 DC 2A 40 00 D6 2A 40 00 D0 2A 40 00 .*@..*@..*@..*@.
00416534 37 10 40 00 CA 2A 40 00 C4 2A 40 00 BE 2A 40 00 7.@..*@..*@..*@.
00416544 B8 2A 40 00 B2 2A 40 00 AC 2A 40 00 A6 2A 40 00 .*@..*@..*@..*@.
00016308 00416308: .rdata:aThechosenone+4 (Synchronized with IDA View-A)

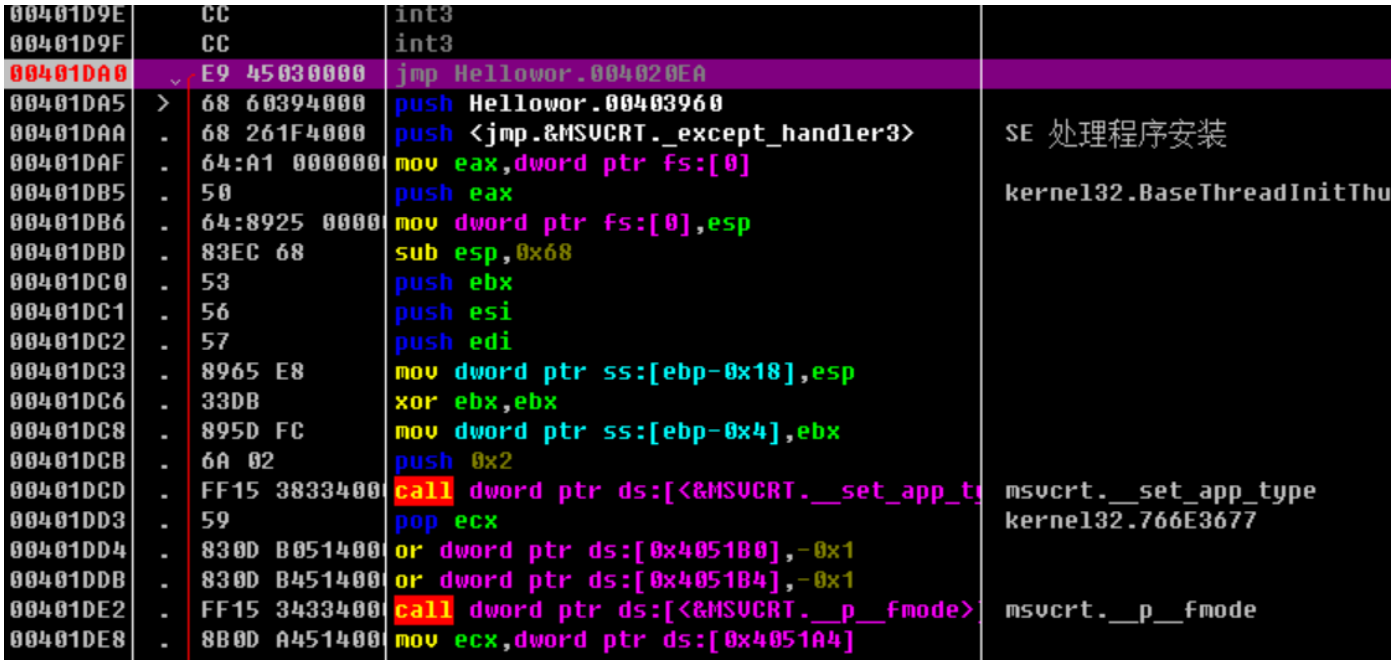
- 改密码:

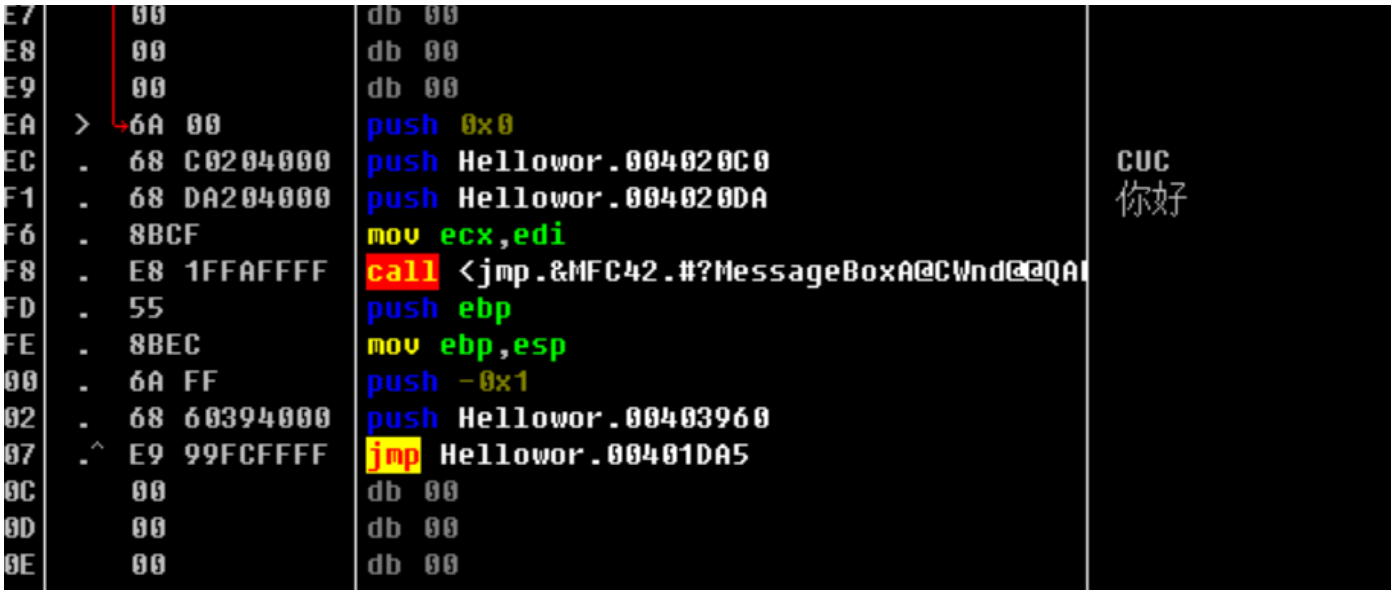
```
)h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
)h: 00 00 00 00 00 00 00 00 00 00 00 00 C3 DC C2 EB ............ÃÜÂë
)h: B4 ED CE F3 00 00 00 00 CA E4 C8 EB B5 C4 C3 DC ´íÎó....ÊäÈëµÄÃÜ
)h: C2 EB D5 FD C8 B7 00 00 00 00 00 00 CC E1 CA BE ÂëÕýÈ·......ÌáÊ¾
)h: 00 00 00 00 68 65 6C 6C 6F 00 00 00 00 00 00 00 ....hello.......
)h: 00 00 00 00 00 00 00 00 5C 63 41 00 54 00 00 00 ........\cA.T...
)h: FF FF 00 00 27 11 40 00 B4 10 40 00 00 00 00 00 ÿÿ..'.@.´.@.....
)h: 14 10 40 00 38 63 41 00 00 00 00 00 00 00 00 00 ..@.8cA.........
)h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
)h: 00 00 00 00 00 00 00 00 00 00 00 00 43 48 65 6C ............CHel
)h: 6C 6F 77 6F 72 64 5F 43 54 46 44 6F 63 00 00 00 loword_CTFDoc...
)h: 00 00 00 00 32 10 40 00 9B 10 40 00 AF 10 40 00 ....2.@.›.@.¯.@.
)h: 46 10 40 00 05 10 40 00 10 2D 40 00 0A 2D 40 00 F.@...@..-@..-@.
)h: E8 2A 40 00 E2 2A 40 00 DC 2A 40 00 D6 2A 40 00 è*@.â*@.Ü*@.Ö*@.
)h: D0 2A 40 00 09 11 40 00 CA 2A 40 00 C4 2A 40 00 Ð*@...@.Ê*@.Ä*@.
)h: BE 2A 40 00 B8 2A 40 00 B2 2A 40 00 AC 2A 40 00 ¾*@.¸*@.²*@.¬*@.
)h: A6 2A 40 00 A0 2A 40 00 9A 2A 40 00 04 2D 40 00 ¦*@. *@.š*@..-@.
)h: FE 2C 40 00 F8 2C 40 00 F2 2C 40 00 EC 2C 40 00 þ,@.ø,@.ò,@.ì,@.
)h: E6 2C 40 00 E0 2C 40 00 DA 2C 40 00 18 11 40 00 æ,@.à,@.Ú,@...@.
)h: D4 2C 40 00 CE 2C 40 00 C8 2C 40 00 C2 2C 40 00 Ô,@.Î,@.È,@.Â,@.
)h: BC 2C 40 00 B6 2C 40 00 B0 2C 40 00 AA 2C 40 00 ¼,@.¶,@.°,@.ª,@.
)h: A4 2C 40 00 9E 2C 40 00 98 2C 40 00 92 2C 40 00 ¤,@.ž,@.˜,@.',@.
)h: 8C 2C 40 00 86 2C 40 00 80 2C 40 00 00 00 00 00 Œ,@.†,@.€,@.....
)h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
)h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
)h: EC 64 41 00 44 00 00 00 FF FF 00 00 C3 10 40 00 ìdA.D...ÿÿ..Ã.@.
)h: 0F 10 40 00 00 00 00 00 F5 10 40 00 70 64 41 00 ..@.....õ.@.pdA.
)h: 11 01 00 00 00 00 00 00 07 E1 00 00 07 E1 00 00 .........á...á..
```

- 输入密码测试：

3.对我们共享的 Helloworld.exe 插入二进制或者汇编代码，弹出 messagebox

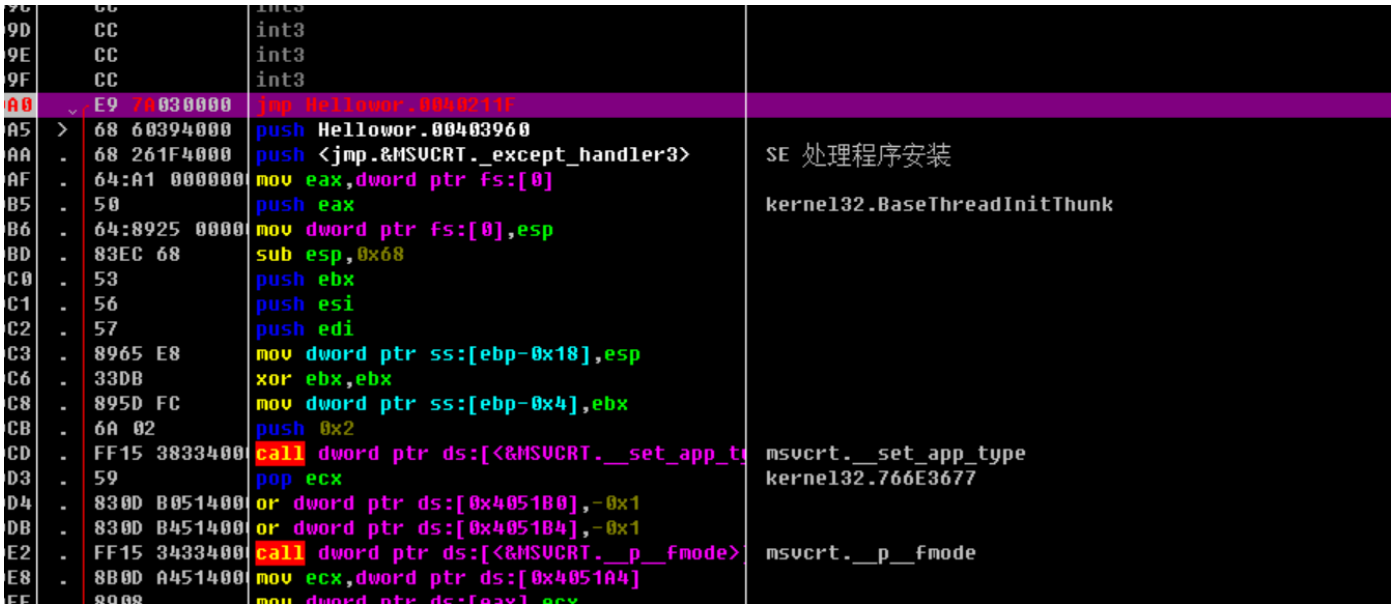
- win10弹不出使用了老师的win7
- 对照着老师所给虚拟机中已经插桩完成的汇编语言进行修改的，首先找到跳转的位置：

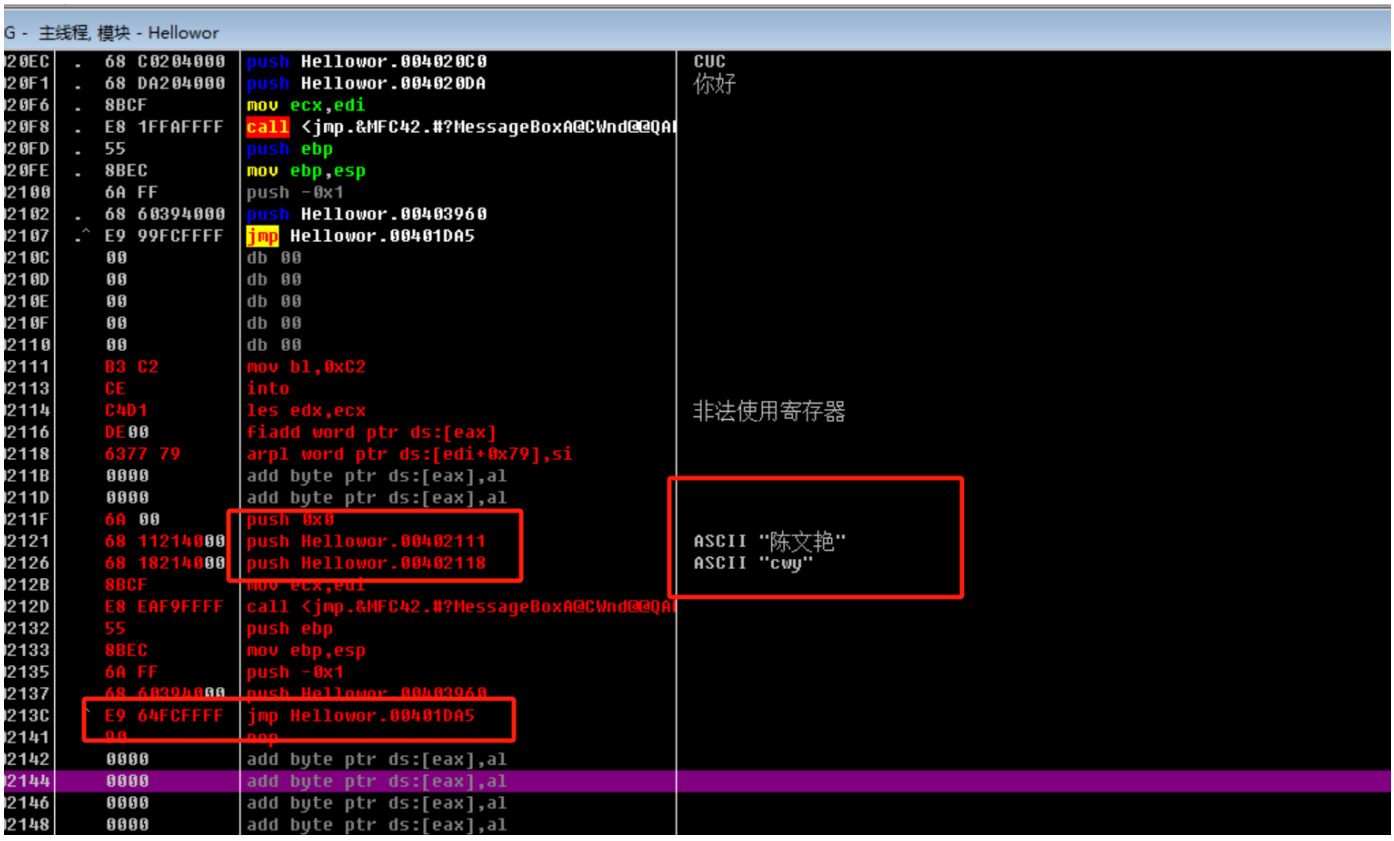




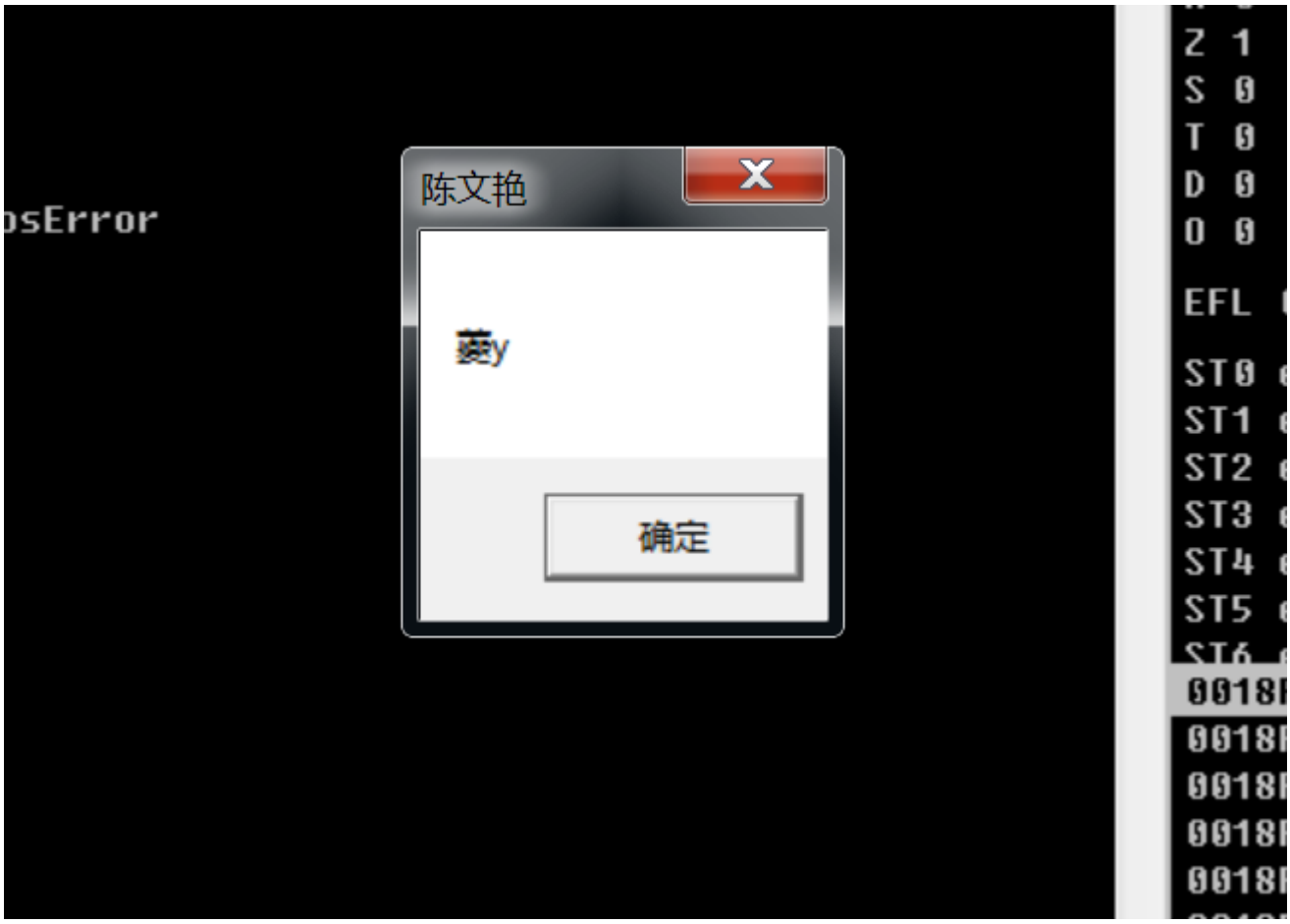
`jmp Hellowor.5G451DA5` 跳转到最后的位置

- 模仿上述代码，在可编写处插入编写了新的字符串以及执行汇编代码的位置，并且修改了一开始跳转的地址，指向了新的汇编代码所在的位置：


9D CC int3
9E CC int3
9F CC int3
A0 E9 7A030000 jmp Hellowor.0040211F
A5 68 60394000 push Hellowor.00403960
AA 68 261F4000 push <jmp.&MSVCRT._except_handler3>
AF 64:A1 000000 mov eax,dword ptr fs:[0]
B5 50 push eax
B6 64:8925 0000 mov dword ptr fs:[0],esp
BD 83EC 68 sub esp,0x68
C0 53 push ebx
C1 56 push esi
C2 57 push edi
C3 8965 E8 mov dword ptr ss:[ebp-0x18],esp
C6 33DB xor ebx,ebx
C8 895D FC mov dword ptr ss:[ebp-0x4],ebx
CB 6A 02 push 0x2
CD FF15 3833400 call dword ptr ds:[<&MSVCRT.__set_app_t
D3 59 pop ecx
D4 830D B051400 or dword ptr ds:[0x4051B0],-0x1
DB 830D B451400 or dword ptr ds:[0x4051B4],-0x1
E2 FF15 3433400 call dword ptr ds:[<&MSVCRT.__p__fmode>]
E8 8B0D A451400 mov ecx,dword ptr ds:[0x4051A4]
SE 处理程序安装
kernel32.BaseThreadInitThunk
msvcrt.__set_app_type
kernel32.766E3677
msvcrt.__p__fmode


G - 主线程, 模块 - Hellowor
20EC 68 C0204000 push Hellowor.004020C0
20F1 68 DA204000 push Hellowor.004020DA
20F6 8BCF mov ecx,edi
20F8 E8 1FFAFFFF call <jmp.&MFC42.#?MessageBoxA@CWnd@@QA
20FD 55 push ebp
20FE 8BEC mov ebp,esp
2100 6A FF push -0x1
2102 68 60394000 push Hellowor.00403960
2107 E9 99FCFFFF jmp Hellowor.00401DA5
210C 00 db 00
210D 00 db 00
210E 00 db 00
210F 00 db 00
2110 00 db 00
2111 B3 C2 mov bl,0xC2
2113 CE into
2114 C4D1 les edx,ecx
2116 DE00 fiadd word ptr ds:[eax]
2118 6377 79 arpl word ptr ds:[edi+0x79],si
211B 0000 add byte ptr ds:[eax],al
211D 0000 add byte ptr ds:[eax],al
211F 6A 00 push 0x0
2121 68 11214000 push Hellowor.00402111
2126 68 18214000 push Hellowor.00402118
212B 8BCF mov ecx,edi
212D E8 EAF9FFFF call <jmp.&MFC42.#?MessageBoxA@CWnd@@QA
2132 55 push ebp
2133 8BEC mov ebp,esp
2135 6A FF push -0x1
2137 68 60394000 push Hellowor.00403960
213C E9 64FCFFFF jmp Hellowor.00401DA5
2141 00 pop
2142 0000 add byte ptr ds:[eax],al
2144 0000 add byte ptr ds:[eax],al
2146 0000 add byte ptr ds:[eax],al
2148 0000 add byte ptr ds:[eax],al
CUC
你好
非法使用寄存器
ASCII "陈文艳"
ASCII "cwy"

- 调试结果：



- 不知道为什么 cwy 前两个乱码成这样，换一下字之后没有这种情况