

XCTF csaw2013reversing2

原创

YenKoc 于 2020-01-28 23:20:38 发布 658 收藏

分类专栏: [XCTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/YenKoc/article/details/104103487>

版权



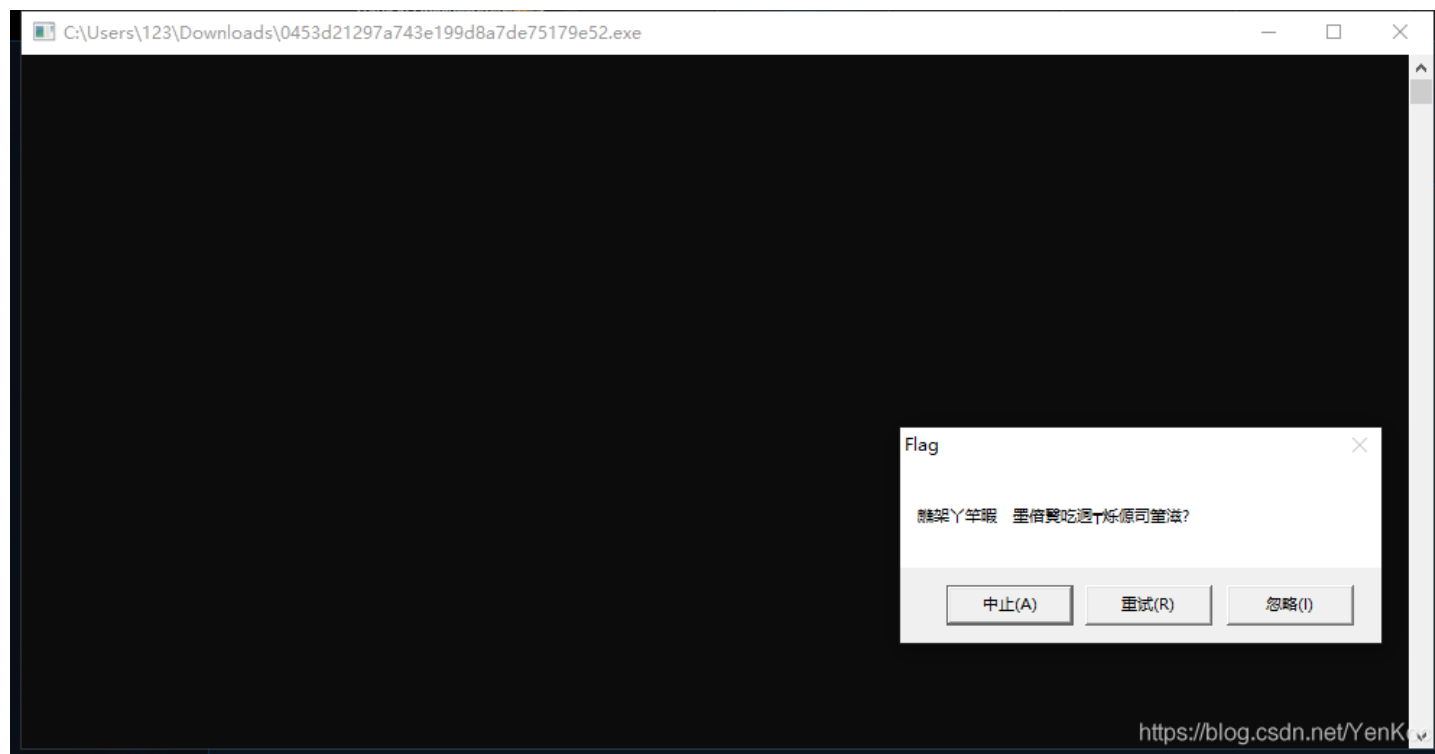
[XCTF 专栏收录该内容](#)

26 篇文章 2 订阅

订阅专栏

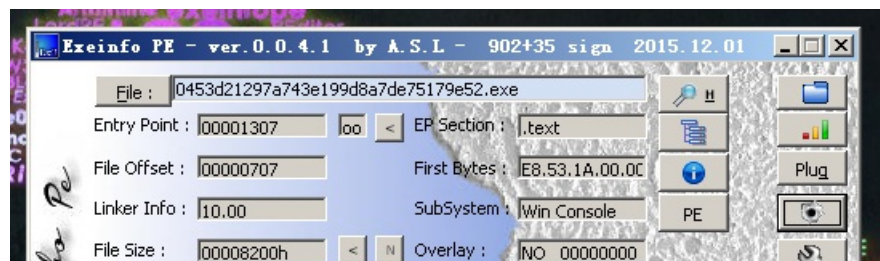
题目描述: 听说运行就能拿到Flag, 不过菜鸡运行的结果不知道为什么是乱码

一.先运行看看。



果然乱码。

二.查壳





三是pe文件，可以拖入od和ida进行动态和静态分析。

1.对主函数进行反编译一下。

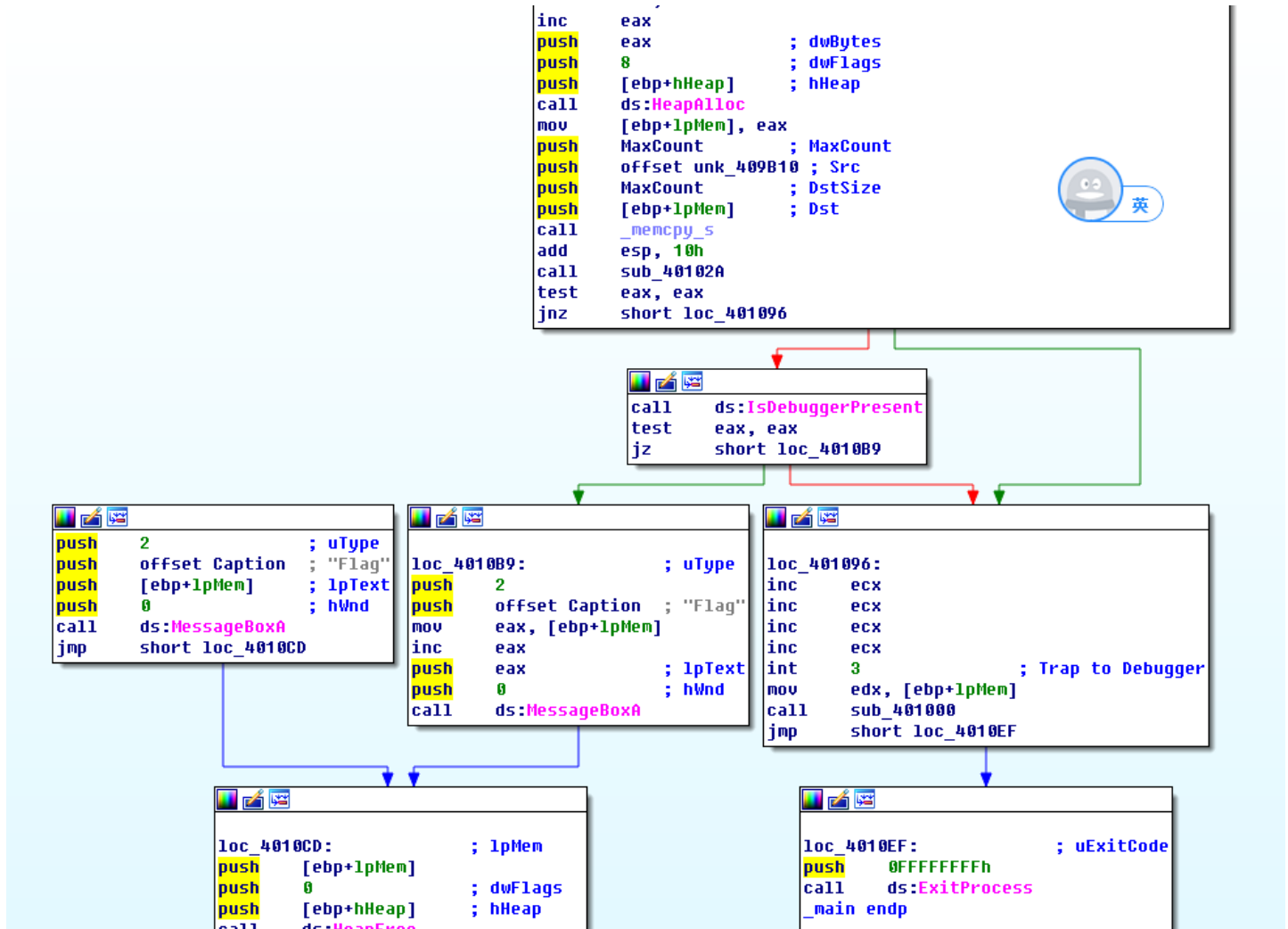
```

1 int __cdecl __noreturn main(int argc, const char **argv, const char **envp)
2 {
3     int v3; // ecx@1
4     LPVOID lpMem; // [sp+8h] [bp-Ch]@1
5     HANDLE hHeap; // [sp+10h] [bp-4h]@1
6
7     hHeap = HeapCreate(0x40000u, 0, 0);
8     lpMem = HeapAlloc(hHeap, 8u, MaxCount + 1);
9     memcpy_s(lpMem, MaxCount, &unk_409B10, MaxCount);
10    if ( sub_40102A() || IsDebuggerPresent() )
11    {
12        __debugbreak();
13        sub_401000(v3 + 4, (int)lpMem);
14        ExitProcess(0xFFFFFFFF);
15    }
16    MessageBoxA(0, (LPCSTR)lpMem + 1, "Flag", 2u);
17    HeapFree(hHeap, 0, lpMem);
18    HeapDestroy(hHeap);
19    ExitProcess(0);
20 }

```

<https://blog.csdn.net/YenKoc>

2.这里可以直接看出代码的逻辑和用意，那个if语句可以解码，如果没进入这步，会直接输出乱码的东西，看看汇编，这里已经利用最大资源了，我们来看看汇编是咋样的。



```

mov [ebp+var_8], eax
push [ebp+hHeap] ; hHeap

```

3.结合着伪代码来看，loc_401096是解码的函数，而loc_4010B9是输出窗口的函数，那么我们只要jmp到解码函数，同时到跳到输出窗口，flag不就解码出来了么。

4.拖入od，中文查找。

```

00401042 - 6A 00      push 0x0
00401044 - 68 00000400 push 0x40000
00401049 - FF15 1060400 call dword ptr ds:[<&KERNEL32.HeapCreate
0040104F - 8945 FC    mov dword ptr ss:[ebp-0x4],eax
00401052 - A1 349B4000 mov eax,dword ptr ds:[0x409B34]
00401057 - 40        inc eax
00401058 - 50        push eax
00401059 - 6A 08     push 0x8
0040105B - FF75 FC    push dword ptr ss:[ebp-0x4]
0040105E - FF15 0460400 call dword ptr ds:[<&KERNEL32.HeapAlloc
00401064 - 8945 F4    mov dword ptr ss:[ebp-0x4],eax
00401067 - FF35 349B400 push dword ptr ds:[0x409B34]
0040106D - 68 109B4000 push 0453d212.00409B10
00401072 - FF35 349B400 push dword ptr ds:[0x409B34]
00401078 - FF75 F4    push dword ptr ss:[ebp-0xC]
0040107B - E8 88000000 call 0453d212.00401108
00401080 - 83C4 10    add esp,0x10
00401083 - E8 A2FFFFFF call 0453d212.0040102A
00401088 - 85C0      test eax,eax
0040108A - 75 0A     jnz short 0453d212.00401096
0040108C - FF15 1460400 call dword ptr ds:[<&KERNEL32.IsDebugger
00401092 - 85C0      test eax,eax
00401094 - 74 23     je short 0453d212.004010B9
00401096 > 41        inc ecx
00401097 - 41        inc ecx
00401098 - 41        inc ecx
00401099 - 41        inc ecx
0040109A - CC        int3
0040109B - 8B55 F4    mov edx,dword ptr ss:[ebp-0xC]
0040109E - E8 5DFFFFFF call 0453d212.00401000
004010A3 - EB 4A     jmp short 0453d212.004010EF
004010A5 - 6A 02     push 0x2
004010A7 - 68 20784000 push 0453d212.00407820
004010AC - FF75 F4    push dword ptr ss:[ebp-0xC]
004010AF - 6A 00     push 0x0
004010B1 - FF15 E460400 call dword ptr ds:[<&USER32.MessageBoxA]
InitialSize = 0x0
Flags = 40000
HeapCreate
$
dwBytes = 0x0
dwFlags = HEAP_ZERO
hHeap = NULL
RtlAllocateHeap
$
$
kernel32.7C839AD8
$
kernel32.7C839AD8
Style = MB_ABORTRETI
Flag
Text = "U巒渡#SUWU
hOwner = NULL
MessageBoxA

```

修改汇编代码。

```

00401078 - FF75 F4    push dword ptr ss:[ebp-0xC]
0040107B - E8 88000000 call 0453d212.00401108
00401080 - 83C4 10    add esp,0x10
00401083 - E8 A2FFFFFF call 0453d212.0040102A
00401088 - 85C0      test eax,eax
0040108A - 75 0A     jnz short 0453d212.00401096
0040108C - FF15 1460400 call dword ptr ds:[<&KERNEL32.IsDebugger
00401092 - 85C0      test eax,eax
00401094 - 74 00     je short 0453d212.00401096
00401096 > 41        inc ecx
00401097 - 41        inc ecx
00401098 - 41        inc ecx
00401099 - 41        inc ecx
0040109A - 90        nop
0040109B - 8B55 F4    mov edx,dword ptr ss:[ebp-0xC]
0040109E - E8 5DFFFFFF call 0453d212.00401000
004010A3 - EB 14     jmp short 0453d212.004010B9
004010A5 - 6A 02     push 0x2
004010A7 - 68 20784000 push 0453d212.00407820
004010AC - FF75 F4    push dword ptr ss:[ebp-0xC]
004010AF - 6A 00     push 0x0
004010B1 - FF15 E460400 call dword ptr ds:[<&USER32.MessageBoxA]
kernel32.7C839AD8
kernel32.7C839AD8
Style = MB_ABORTRETI
Flag
Text = "U巒渡#SUWU
hOwner = NULL
MessageBoxA

```

```

-UNORM D3E0 00714480 004C004A
+UNORM 004A 00000000 00714480

```



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)