XCTF GAME

原创

YenKoc 于 2020-01-15 11:42:17 发布 609 收藏

分类专栏： XCTF

本文链接：https://blog.csdn.net/YenKoc/article/details/103986214

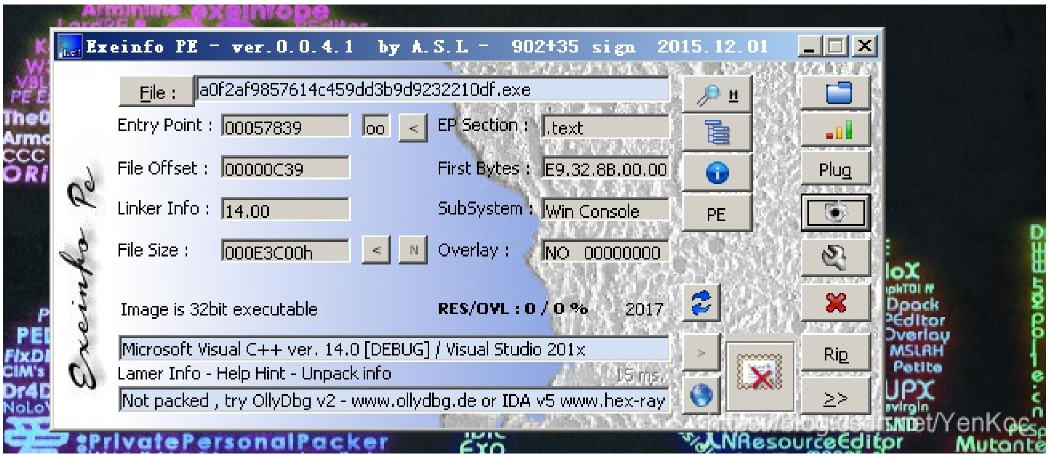
XCTF 专栏收录该内容

26 篇文章 2 订阅

订阅专栏

首先这题有两种解法，一种是使用ida查看伪代码直接写exp跑出flag，另外一种是调试，因为最近在学调试，刚好用于实战上了。

一.查壳



Exeinfo PE - ver.0.0.4.1 by A.S.L - 902+35 sign 2015.12.01

File : a0f2af9857614c459dd3b9d9232210df.exe

Entry Point : 00057839 oo

EP Section : .text

File Offset : 00000C39

First Bytes : E9.32.8B.00.00

Linker Info : 14.00

SubSystem : Win Console

File Size : 000E3C00h

Overlay : NO 00000000

Image is 32bit executable

RES/OVL : 0 / 0 % 2017

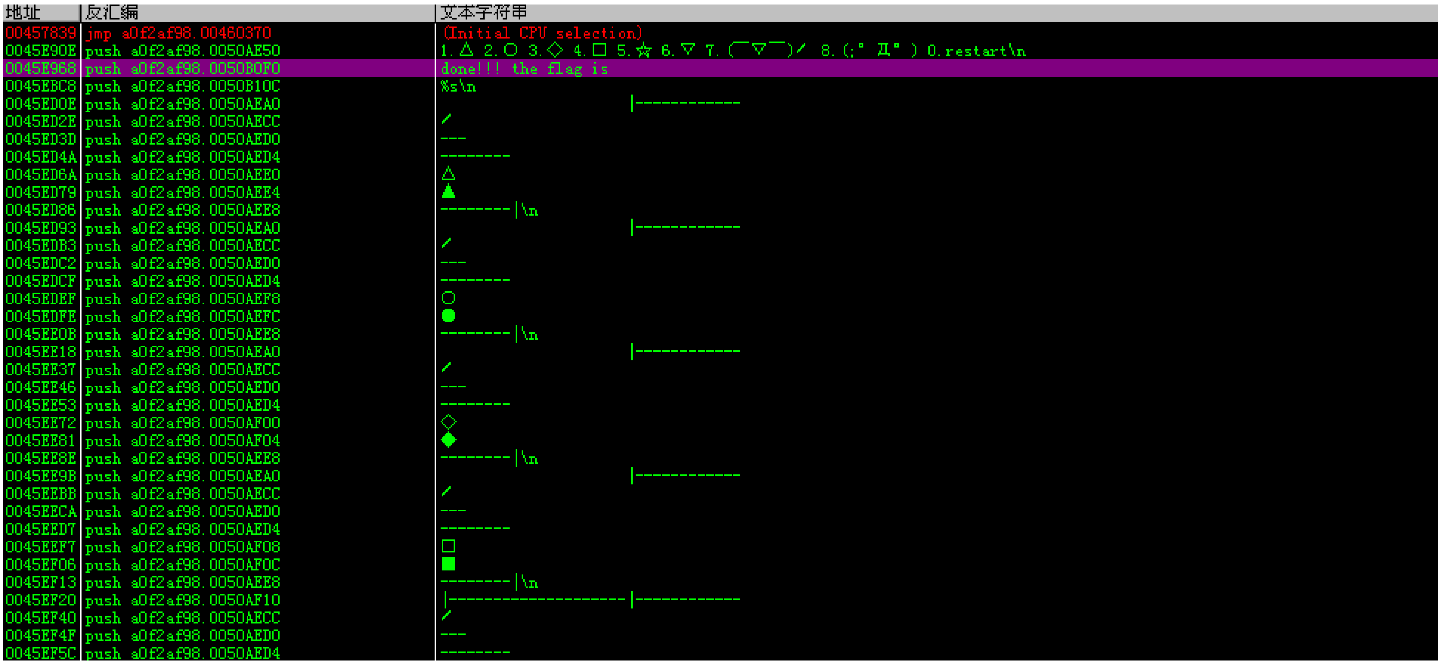
Microsoft Visual C++ ver. 14.0 [DEBUG] / Visual Studio 201x

Lamer Info - Help Hint - Unpack info 15 ms.

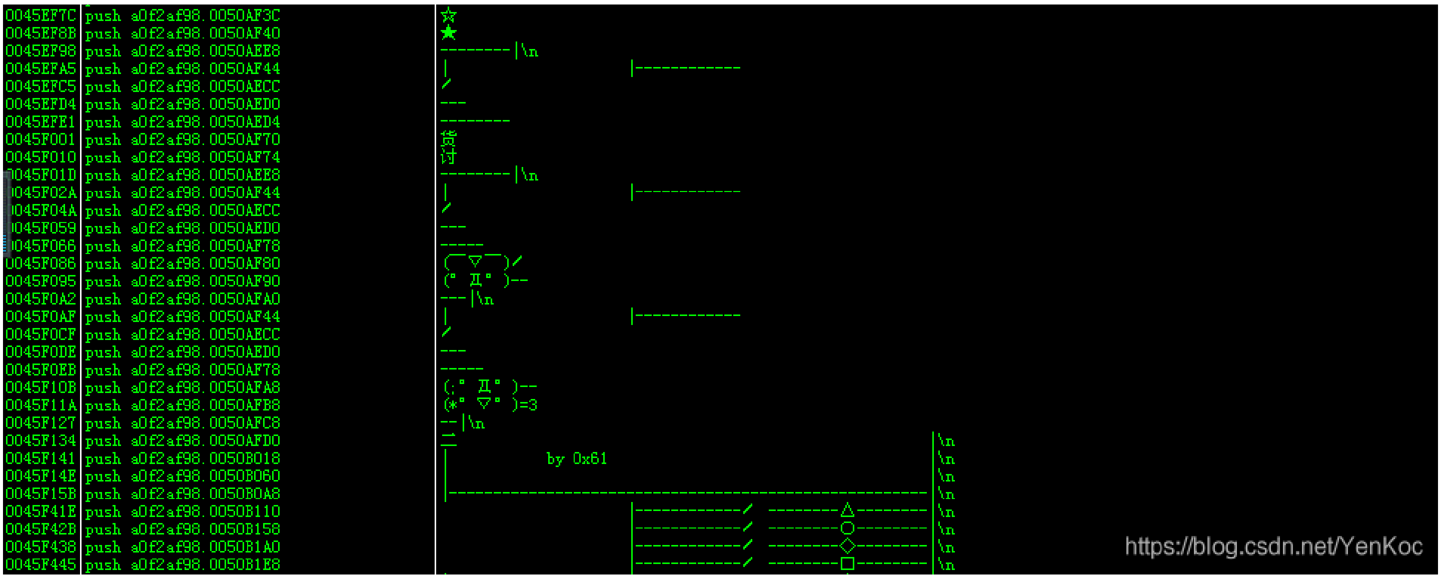
Not packed , try OllyDbg v2 - www.ollydbg.de or IDA v5 www.hex-ray

二.32位文件拖入od动态调试

先找到game的主要函数，插件中文智能搜索一下所有的字符串。

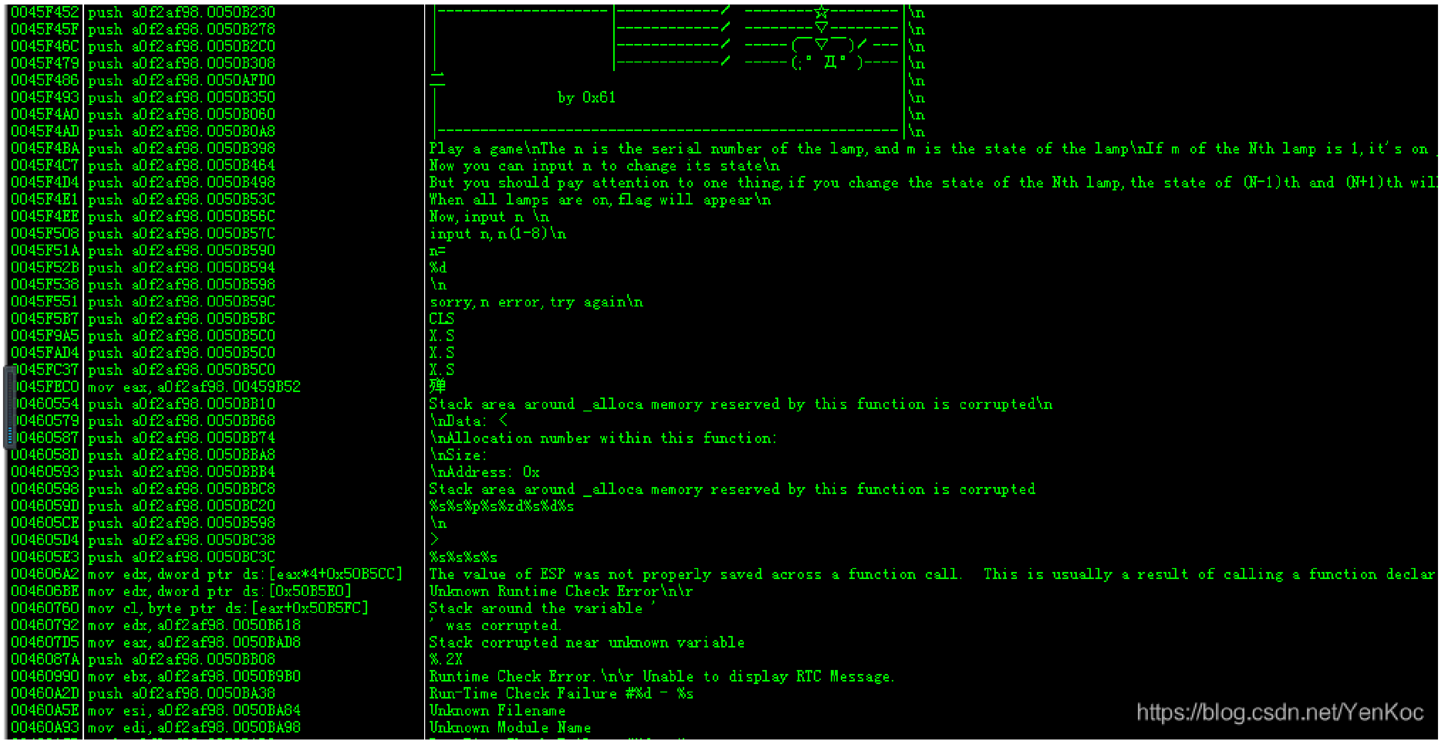


```
地址     |反汇编                        |文本字符串
00457839 |jmp  a0f2af98.00460370        |(Initial CPU selection)
0045E90E |push a0f2af98.0050AE50        |1.△ 2.○ 3.◇ 4.□ 5.☆ 6.▽ 7.(￣▽￣)ノ 8.(;° Д° ) 0.restart\n
0045E968 |push a0f2af98.0050B0F0        |done!!! the flag is
0045EBC8 |push a0f2af98.0050B10C        |%s\n
0045ED0E |push a0f2af98.0050AEA0        |                |------------
0045ED2E |push a0f2af98.0050AECC        |/
0045ED3D |push a0f2af98.0050AED0        |---
0045ED4A |push a0f2af98.0050AED4        |--------
0045ED6A |push a0f2af98.0050AEE0        |△
0045ED79 |push a0f2af98.0050AEE4        |▲
0045ED86 |push a0f2af98.0050AEE8        |--------|\n
0045ED93 |push a0f2af98.0050AEA0        |                |------------
0045EDB3 |push a0f2af98.0050AECC        |/
0045EDC2 |push a0f2af98.0050AED0        |---
0045EDCF |push a0f2af98.0050AED4        |--------
0045EDEF |push a0f2af98.0050AEF8        |○
0045EDFE |push a0f2af98.0050AEFC        |●
0045EE0B |push a0f2af98.0050AEE8        |--------|\n
0045EE18 |push a0f2af98.0050AEA0        |                |------------
0045EE37 |push a0f2af98.0050AECC        |/
0045EE46 |push a0f2af98.0050AED0        |---
0045EE53 |push a0f2af98.0050AED4        |--------
0045EE72 |push a0f2af98.0050AF00        |◇
0045EE81 |push a0f2af98.0050AF04        |◆
0045EE8E |push a0f2af98.0050AEE8        |--------|\n
0045EE9B |push a0f2af98.0050AEA0        |                |------------
0045EEBB |push a0f2af98.0050AECC        |/
0045EECA |push a0f2af98.0050AED0        |---
0045EED7 |push a0f2af98.0050AED4        |--------
0045EEF7 |push a0f2af98.0050AF08        |□
0045EF06 |push a0f2af98.0050AF0C        |■
0045EF13 |push a0f2af98.0050AEE8        |--------|\n
0045EF20 |push a0f2af98.0050AF10        ||----------------|------------
0045EF40 |push a0f2af98.0050AECC        |/
0045EF4F |push a0f2af98.0050AED0        |---
0045EF5C |push a0f2af98.0050AED4        |--------
```



```
0045EF7C push a0f2af98.0050AF3C   ☆
0045EF8B push a0f2af98.0050AF40   ★
0045EF98 push a0f2af98.0050AEE8   ---------|\n
0045EFA5 push a0f2af98.0050AF44   |                      |------------
0045EFC5 push a0f2af98.0050AECC   /
0045EFD4 push a0f2af98.0050AED0   ---
0045EFE1 push a0f2af98.0050AED4   ---------
0045F001 push a0f2af98.0050AF70   货
0045F010 push a0f2af98.0050AF74   讨
0045F01D push a0f2af98.0050AEE8   ---------|\n
0045F02A push a0f2af98.0050AF44   |                      |------------
0045F04A push a0f2af98.0050AECC   /
0045F059 push a0f2af98.0050AED0   ---
0045F066 push a0f2af98.0050AF78   -----
0045F086 push a0f2af98.0050AF80   (￣▽￣)/
0045F095 push a0f2af98.0050AF90   (° Д° )--
0045F0A2 push a0f2af98.0050AFA0   ---|\n
0045F0AF push a0f2af98.0050AF44   |                      |------------
0045F0CF push a0f2af98.0050AECC   /
0045F0DE push a0f2af98.0050AED0   ---
0045F0EB push a0f2af98.0050AF78   -----
0045F10B push a0f2af98.0050AFA8   (;° Д° )--
0045F11A push a0f2af98.0050AFB8   (*° ▽° )=3
0045F127 push a0f2af98.0050AFC8   --|\n
0045F134 push a0f2af98.0050AFD0   二                                                        |\n
0045F141 push a0f2af98.0050B018   |            by 0x61                                     |\n
0045F14E push a0f2af98.0050B060   |                                                        |\n
0045F15B push a0f2af98.0050B0A8   |--------------------------------------------------------|\n
0045F41E push a0f2af98.0050B110                        |------------/  --------△--------|\n
0045F42B push a0f2af98.0050B158                        |------------/  --------○--------|\n
0045F438 push a0f2af98.0050B1A0                        |------------/  --------◇--------|\n
0045F445 push a0f2af98.0050B1E8                        |------------/  --------□--------|\n
```

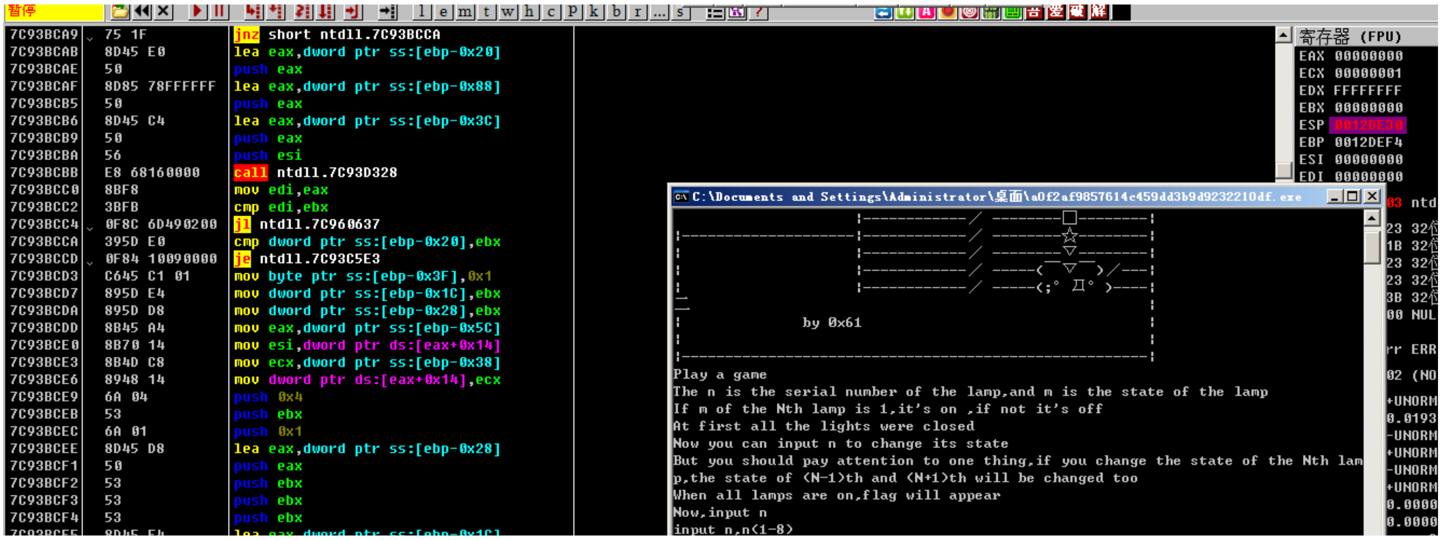
https://blog.csdn.net/YenKoc



```
0045F452 push a0f2af98.0050B230   |--------------------|------------/  --------☆--------|\n
0045F45F push a0f2af98.0050B278   |                    |------------/  --------▽--------|\n
0045F46C push a0f2af98.0050B2C0   |                    |------------/  -----(￣▽￣)/---|\n
0045F479 push a0f2af98.0050B308   |                    |------------/  -----(;° Д° )----|\n
0045F486 push a0f2af98.0050AFD0   二                                                    |\n
0045F493 push a0f2af98.0050B350   |            by 0x61                                 |\n
0045F4A0 push a0f2af98.0050B060   |                                                    |\n
0045F4AD push a0f2af98.0050B0A8   |----------------------------------------------------|\n
0045F4BA push a0f2af98.0050B398   Play a game\nThe n is the serial number of the lamp, and m is the state of the lamp\nIf m of the Nth lamp is 1, it's on
0045F4C7 push a0f2af98.0050B464   Now you can input n to change its state\n
0045F4D4 push a0f2af98.0050B498   But you should pay attention to one thing, if you change the state of the Nth lamp, the state of (N-1)th and (N+1)th wil
0045F4E1 push a0f2af98.0050B53C   When all lamps are on, flag will appear\n
0045F4EE push a0f2af98.0050B56C   Now, input n \n
0045F508 push a0f2af98.0050B57C   input n, n(1-8)\n
0045F51A push a0f2af98.0050B590   n=
0045F52B push a0f2af98.0050B594   %d
0045F538 push a0f2af98.0050B598   \n
0045F551 push a0f2af98.0050B59C   sorry, n error, try again\n
0045F5B7 push a0f2af98.0050B5BC   CLS
0045F9A5 push a0f2af98.0050B5C0   X.S
0045FAD4 push a0f2af98.0050B5C0   X.S
0045FC37 push a0f2af98.0050B5C0   X.S
0045FEC0 mov eax, a0f2af98.00459B52   弹
00460554 push a0f2af98.0050BB10   Stack area around _alloca memory reserved by this function is corrupted\n
00460579 push a0f2af98.0050BB68   \nData: <
00460587 push a0f2af98.0050BB74   \nAllocation number within this function:
0046058D push a0f2af98.0050BBA8   \nSize:
00460593 push a0f2af98.0050BBB4   \nAddress: 0x
00460598 push a0f2af98.0050BBC8   Stack area around _alloca memory reserved by this function is corrupted
0046059D push a0f2af98.0050BC20   %s%s%p%s%zd%s%d%s
004605CE push a0f2af98.0050B598   \n
004605D4 push a0f2af98.0050BC38   >
004605E3 push a0f2af98.0050BC3C   %s%s%s%s
004606A2 mov edx, dword ptr ds:[eax*4+0x50B5CC]   The value of ESP was not properly saved across a function call.  This is usually a result of calling a function declar
004606BE mov edx, dword ptr ds:[0x50B5E0]   Unknown Runtime Check Error\n\r
00460760 mov cl, byte ptr ds:[eax+0x50B5FC]   Stack around the variable '
00460792 mov edx, a0f2af98.0050B618   ' was corrupted.
004607D5 mov eax, a0f2af98.0050BAD8   Stack corrupted near unknown variable
0046087A push a0f2af98.0050BB08   %.2X
00460990 mov ebx, a0f2af98.0050B9B0   Runtime Check Error.\n\r Unable to display RTC Message.
00460A2D push a0f2af98.0050BA38   Run-Time Check Failure #%d - %s
00460A5E mov esi, a0f2af98.0050BA84   Unknown Filename
00460A93 mov edi, a0f2af98.0050BA98   Unknown Module Name
```

https://blog.csdn.net/YenKoc

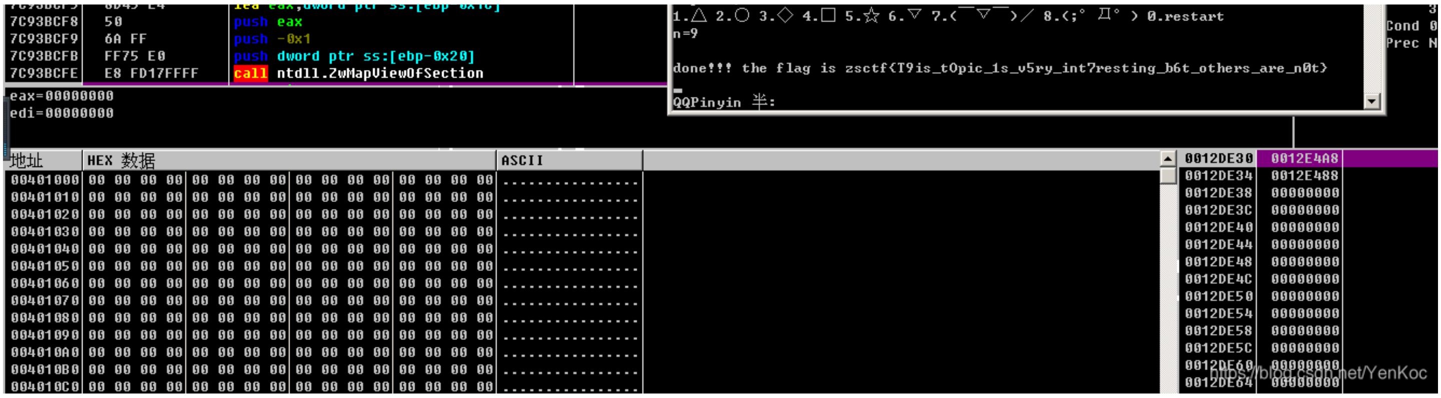
找到了，那个input :的字符串，就是我们需要找到game的函数，同时在第一张图片中也找到了一个done flag is，猜测是正确后会得到flag，那么只要修改汇编代码，直接跳转到done这个的函数，不就做出来了吗。



```
7C93BCA9  75 1F           jnz short ntdll.7C93BCCA
7C93BCAB  8D45 E0         lea eax,dword ptr ss:[ebp-0x20]
7C93BCAE  50              push eax
7C93BCAF  8D85 78FFFFFF   lea eax,dword ptr ss:[ebp-0x88]
7C93BCB5  50              push eax
7C93BCB6  8D45 C4         lea eax,dword ptr ss:[ebp-0x3C]
7C93BCB9  50              push eax
7C93BCBA  56              push esi
7C93BCBB  E8 68160000     call ntdll.7C93D328
7C93BCC0  8BF8            mov edi,eax
7C93BCC2  3BFB            cmp edi,ebx
7C93BCC4  0F8C 6D490200   jl ntdll.7C960637
7C93BCCA  395D E0         cmp dword ptr ss:[ebp-0x20],ebx
7C93BCCD  0F84 10090000   je ntdll.7C93C5E3
7C93BCD3  C645 C1 01      mov byte ptr ss:[ebp-0x3F],0x1
7C93BCD7  895D E4         mov dword ptr ss:[ebp-0x1C],ebx
7C93BCDA  895D D8         mov dword ptr ss:[ebp-0x28],ebx
7C93BCDD  8B45 A4         mov eax,dword ptr ss:[ebp-0x5C]
7C93BCE0  8B70 14         mov esi,dword ptr ds:[eax+0x14]
7C93BCE3  8B4D C8         mov ecx,dword ptr ss:[ebp-0x38]
7C93BCE6  8948 14         mov dword ptr ds:[eax+0x14],ecx
7C93BCE9  6A 04           push 0x4
7C93BCEB  53              push ebx
7C93BCEC  6A 01           push 0x1
7C93BCEE  8D45 D8         lea eax,dword ptr ss:[ebp-0x28]
7C93BCF1  50              push eax
7C93BCF2  53              push ebx
7C93BCF3  53              push ebx
7C93BCF4  53              push ebx
```

```
寄存器 (FPU)
EAX 00000000
ECX 00000001
EDX FFFFFFFF
EBX 00000000
ESP 0012DE30
EBP 0012DEF4
ESI 00000000
EDI 00000000
```

```
C:\Documents and Settings\Administrator\桌面\a0f2af9857614c459dd3b9d9232210df.exe
                    |-------------/  --------□--------|
|-------------------|-------------/  --------☆--------|
|                   |-------------/  --------▽--------|
|                   |-------------/  -----(￣▽￣)/---|
|                   |-------------/  -----(;° Д° )----|
二                                                    |
|          by 0x61                                    |
|                                                     |
|-----------------------------------------------------|
Play a game
The n is the serial number of the lamp,and m is the state of the lamp
If m of the Nth lamp is 1,it's on ,if not it's off
At first all the lights were closed
Now you can input n to change its state
But you should pay attention to one thing,if you change the state of the Nth lam
p,the state of (N-1)th and (N+1)th will be changed too
When all lamps are on,flag will appear
Now,input n
input n,n(1-8)
```



```
7C93BCF8   50          push eax
7C93BCF9   6A FF       push -0x1
7C93BCFB   FF75 E0     push dword ptr ss:[ebp-0x20]
7C93BCFE   E8 FD17FFFF call ntdll.ZwMapViewOfSection
eax=00000000
edi=00000000
```

```
1.△ 2.○ 3.◇ 4.□ 5.☆ 6.▽ 7.(￣▽￣)/ 8.(;° 口° ) 0.restart
n=9

done!!! the flag is zsctf{T9is_t0pic_1s_v5ry_int7resting_b6t_others_are_n0t}
QQPinyin 半:
```

```
地址      HEX 数据                                         ASCII
00401000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00401010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00401020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00401030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00401040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00401050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00401060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00401070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00401080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00401090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004010A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004010B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004010C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
0012DE30  0012E4A8
0012DE34  0012E488
0012DE38  00000000
0012DE3C  00000000
0012DE40  00000000
0012DE44  00000000
0012DE48  00000000
0012DE4C  00000000
0012DE50  00000000
0012DE54  00000000
0012DE58  00000000
0012DE5C  00000000
0012DE60  00000000
0012DE64  00000000
```

这里调试过程真的算简单的一批了，单步调试一步一步，之后jmp一下函数，结束了。