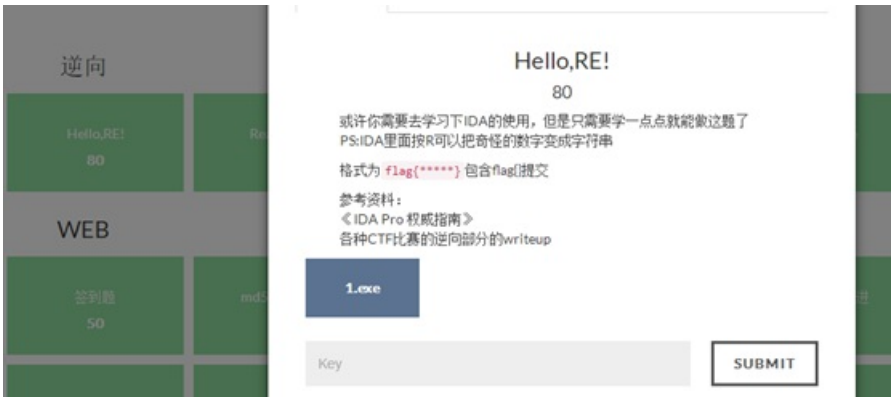
南邮CTF逆向题第一道Hello,RE!解题思路

原创

iqiqiya 于 2017-12-23 11:18:46 发布 4729 收藏 2
分类专栏： ------南邮CTF 我的CTF进阶之路 文章标签： 南邮CTF writeup 逆向


------南邮CTF 同时被 2 个专栏收录
6 篇文章 0 订阅
订阅专栏
我的CTF进阶之路
108 篇文章 18 订阅
订阅专栏

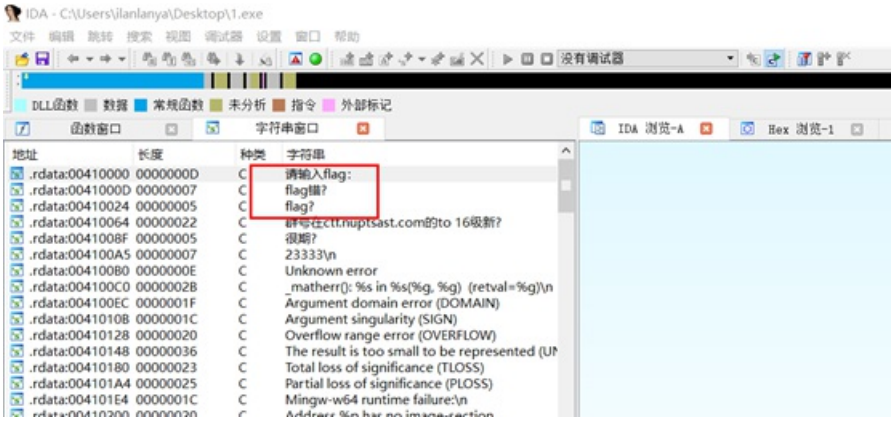
首先可以看到提示如下



我还是查了一下 无壳

提示用IDA

那我们就载入 shift+f12查找字符串



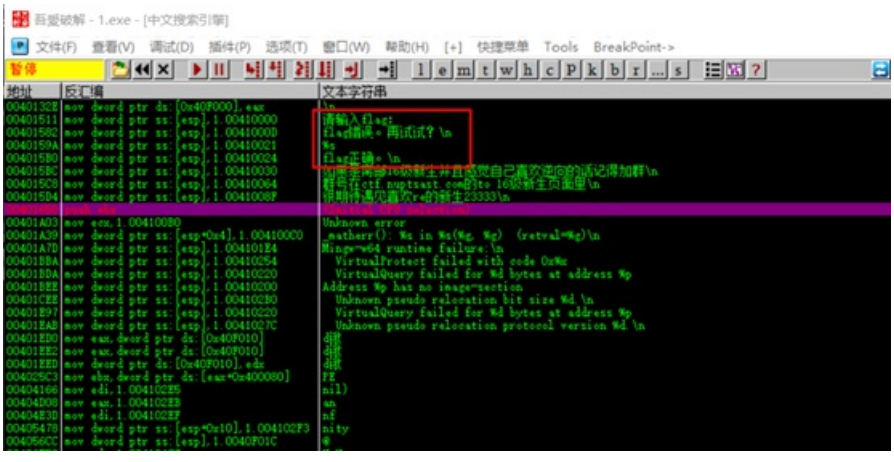
双击进入 在右侧窗口接着双击 然后f5看到了伪代码 于是点击字符串全按R即可

IDA 浏览-A | 伪代码-A | Hex 浏览-1 | 结构体

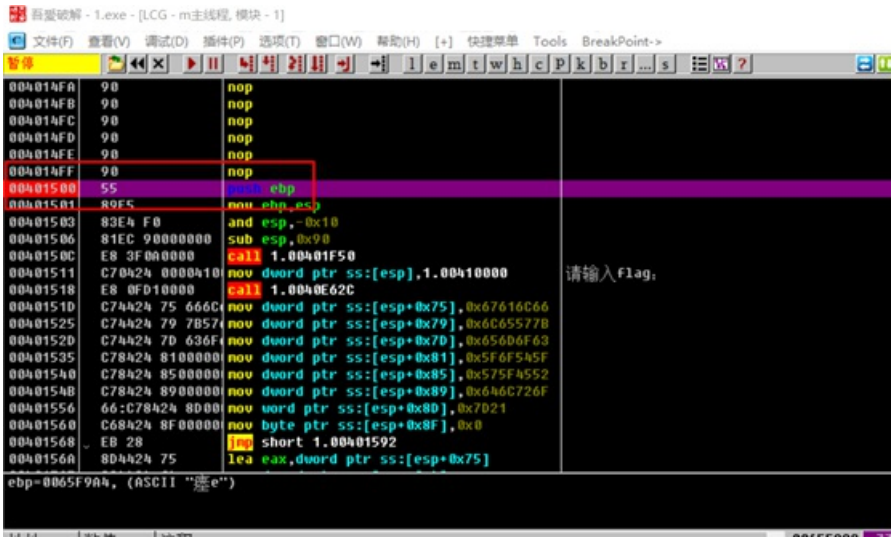
```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  _BYTE v4[3]; // [sp+11h] [bp-7Fh]@2
  signed int v5; // [sp+75h] [bp-1Bh]@1
  signed int v6; // [sp+79h] [bp-17h]@1
  signed int v7; // [sp+7Dh] [bp-13h]@1
  signed int v8; // [sp+81h] [bp-Fh]@1
  signed int v9; // [sp+85h] [bp-Bh]@1
  signed int v10; // [sp+89h] [bp-7h]@1
  signed __int16 v11; // [sp+8Dh] [bp-3h]@1
  char v12; // [sp+8Fh] [bp-1h]@1

  __main();
  printf("请输入flag：");
  v5 = 'galf';
  v6 = 'leW{';
  v7 = 1701670755;
  v8 = 1601131615;
  v9 = 1465861458;
  v10 = 1684828783;
  v11 = 32033;
  v12 = 0;
  while ( scanf("%s", v4) != -1 && strcmp(v4, (const char *)&v5) )
    printf("flag错误。再试试？\n");
  printf("flag正确。\n");
  printf("如果是南邮16级新生并且感觉自己喜欢逆向的话记得加群\n");
  printf("群号在ctf.nuptsast.com的to 16级新生页面里\n");
  printf("很期待遇见喜欢re的新生23333\n");
  getchar();
  getchar();
  return 0;
}
```

```
  __main();
  printf("请输入flag：");
  v5 = 'galf';
  v6 = 'leW{';
  v7 = 'emoc';
  v8 = '_oT_';
  v9 = 'W_ER';
  v10 = 'dlro';
  v11 = '}!';
  v12 = 0;
```

我再用OD试一下

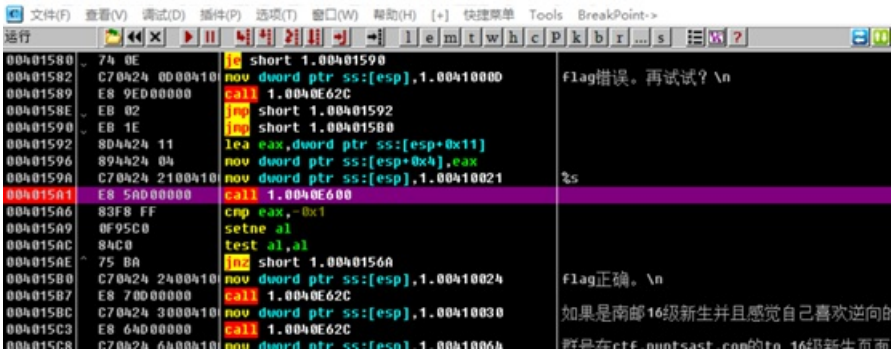


段首F2下断

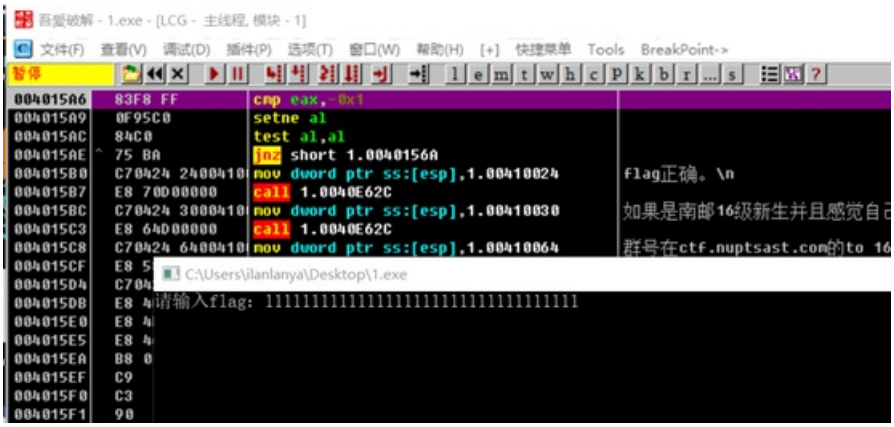


F9运行 段下来后接着单步

走到这个call处

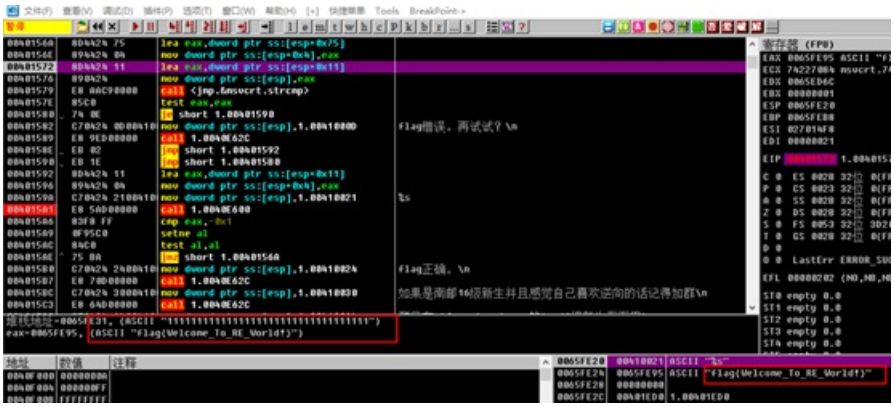


输入假码 回车



接着慢慢向下单步走

没走两步 就发现flag


lea eax,dword ptr ss:[esp+0x75]
mov dword ptr ss:[esp+0x4],eax
lea eax,dword ptr ss:[esp+0x11]
mov dword ptr ss:[esp],eax
call <jmp.&msvcrt.strcmp>
test eax,eax
jne short 1.00401590
mov dword ptr ss:[esp],1.00A10000
call 1.00ADE62C
jmp short 1.00401592
jmp short 1.00401580
lea eax,dword ptr ss:[esp+0x11]
mov dword ptr ss:[esp+0x4],eax
mov dword ptr ss:[esp],1.00A10021
call 1.00ADE640
cmp eax,-0x1
setne al
test al,al
jne short 1.0040156A
mov dword ptr ss:[esp],1.00A10024
call 1.00ADE62C
mov dword ptr ss:[esp],1.00A10038
call 1.00ADE62C
flag错误，再试试？\n
%s
flag正确。\n
如果是南邮16级新生并且感觉自己喜欢逆向的话记得加群\n
寄存器 (FPU)
EAX 0065FE95 ASCII "Flag{Welcome_To_RE_World!}"
ECX 7422708A msvcrt.7
EDX 0065ED4C
EBX 00000001
ESP 0065FE20
EBP 0065FE88
ESI 027D14F8
EDI 00000021
EIP 00401580 1.00401580
C 0 ES 0028 32位 0(FF
P 0 CS 0023 32位 0(FF
A 0 SS 0028 32位 0(FF
Z 0 DS 0028 32位 0(FF
S 0 FS 0053 32位 3D2
T 0 GS 0028 32位 0(FF
D 0
O 0 LastErr ERROR_SU
EFL 00000202 (NO,NB,NE
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
eax=0065FE95, (ASCII "Flag{Welcome_To_RE_World!}")
地址 数值 注释
0065FE20 00A10021 ASCII "!"
0065FE24 0065FE95 ASCII "Flag{Welcome_To_RE_World!}"
0065FE28 00000000
0065FE2C 00401ED0 1.00401ED0