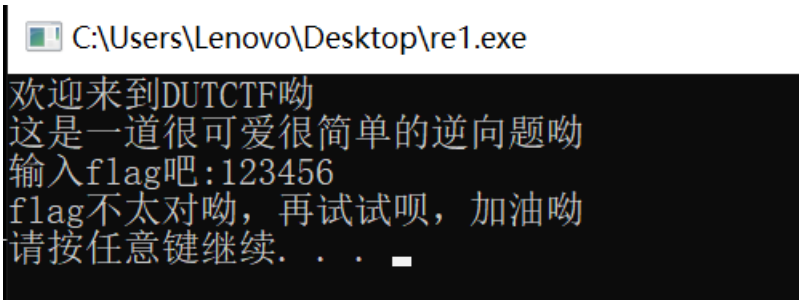
攻防世界reverse新手练习区re1

原创

仲月二八 于 2021-07-23 15:40:59 发布 50 收藏

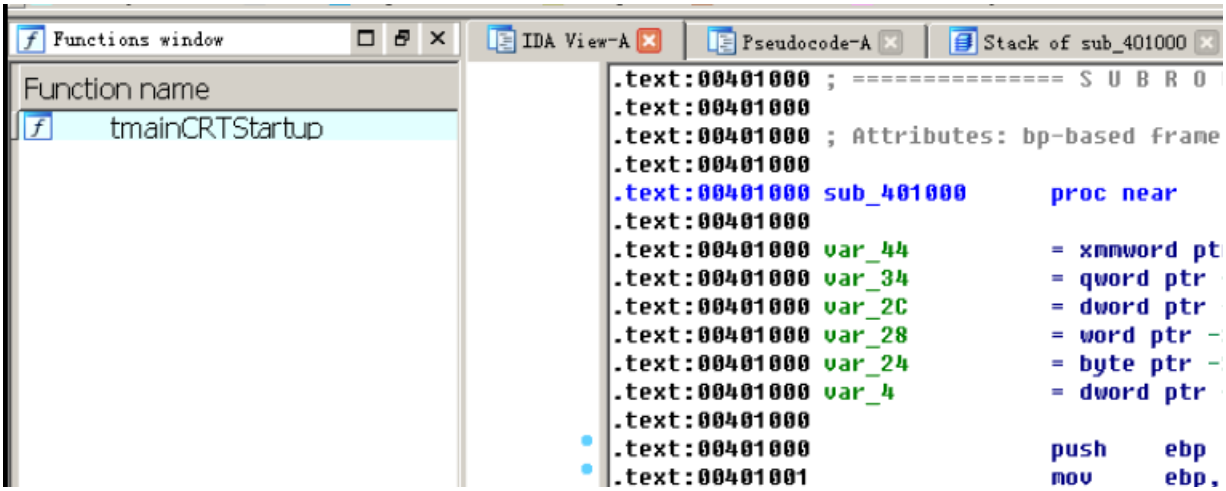
攻防世界reverse新手练习区re1

打开题目下载附件是一个exe文件，运行一下结果如下



根据上图可知需要输入正确的flag，用exeinfo pe查看exe程序详细信息，该文件没有加壳，是32位的。

于是用32位ida打开，按ctrl加F建查找main函数，没有找到



于是直接点进第一个函数sub401000，双击sub401000函数，按F5查看C代码

```
1 int sub_401000()
2 {
3   char v0; // ST10_1@1
4   char v1; // ST0C_1@1
5   int v2; // eax@1
6   __int128 v4; // [sp+0h] [bp-44h]@1
7   __int64 v5; // [sp+10h] [bp-34h]@1
8   int v6; // [sp+18h] [bp-2Ch]@1
9   __int16 v7; // [sp+1Ch] [bp-28h]@1
10  char v8; // [sp+20h] [bp-24h]@1
11
12  _mm_storeu_si128((__m128i *)&v4, _mm_loadu_si128((const __m128i *)&xmmword_413E34));
13  v6 = 0;
14  _mm_storel_epi64((__m128i *)&v5, _mm_loadl_epi64((const __m128i *)&qword_413E44));
15  v7 = 0;
16  sub_40127B((int)"欢迎来到DUTCTF呦\n", v4);
17  sub_40127B((int)"这是一道很可爱很简单的逆向题呦\n", v0);
18  sub_40127B((int)"输入flag吧:", v1);
19  sub_4010D1("%s", &v8);
20  v2 = strcmp((const char *)&v4, &v8);
21  if ( v2 )
22    v2 = -(v2 < 0) | 1;
23  if ( v2 )
24    sub_40127B((int)"flag不太对呦，再试试呗，加油呦\n", v4);
25  else
26    sub_40127B((int)"flag get√\n", v4);
27  sub_401171("pause");
28  return 0;
```

可以看出上图就是该程序的主要代码，第12行的`_mm_storeu_si128`函数作用是将`xmmword_413E34`的值赋给v4；第19行输入的值为v8；20行比较v4和v8的值并将结果赋给v2，若v4与v8相等则v2的值为0，否则为1；21到26行的几个if条件，若v2为1则输出`"flag不太对呦，再试试呗，加油呦"`，若v2位0则输出`"flag getV"`。
通过上述分析可知，只要v8与v4的值相等即可，即v8与`xmmword_413E34`相等，双击`xmmword_413E34`

```
.rdata:00413E33                 align 4
.rdata:00413E34 xmmword_413E34  xmmword 3074656D30633165577B465443545544h
.rdata:00413E34                                         ; DATA XREF: sub_40
.rdata:00413E44 qword_413E44    dq 7D4654435455544h     ; DATA XREF: sub_40
.rdata:00413E4C aNDutctf        db '欢迎来到DUTCTF呦',0Ah    ; DATA XREF: s
.rdata:00413E4C                 db 0
.rdata:00413E5E                 align 10h
.rdata:00413E60 aTOECT          db '这是一道很可爱很简单的逆向题呦',0Ah ; D
.rdata:00413E60                 db 0
.rdata:00413E80 aFIflag         db '输入flag吧:',0          ; DATA XREF: sub
.rdata:00413E8C aS              db '%s',0                   ; DATA XREF: sub_40
.rdata:00413E8F                 align 10h
.rdata:00413E90 aFlagGetb       db 'flag get√',0Ah      ; DATA XREF: sub_4
.rdata:00413E90                 db 0
.rdata:00413E9C aFlagLGmGm      db 'flag不太对呦，再试试呗，加油呦',0Ah
```

在上图两个数字上按R键，得到字符如下

```
.rdata:00413E34 xmmword_413E34  xmmword '0tem0c1eW{FTCTUD' ; DATA XREF:
.rdata:00413E44 qword_413E44    dq '}FTCTUD'              ; DATA XREF: sul
.rdata:00413E4C aNDutctf        db '欢迎来到DUTCTF呦',0Ah     ; DATA XREI
.rdata:00413E4C                 db 0
.rdata:00413E5E                 align 10h
.rdata:00413E60 aTOECT          db '这是一道很可爱很简单的逆向题呦',0Ah
.rdata:00413E60                 db 0
.rdata:00413E80 aFIflag         db '输入flag吧:',0          ; DATA XREF:
.rdata:00413E8C aS              db '%s',0                 ; DATA XREF: sul
.rdata:00413E8F                 align 10h
.rdata:00413E90 aFlagGetb       db 'flag get√',0Ah        ; DATA XREF: s
.rdata:00413E90                 db 0
.rdata:00413E9C aFlagLGmGm      db 'flag不太对呦，再试试呗，加油呦',0Ah
```

得到真确的flag，由于这里是小端存储，正确flag为`DUTCTF{We1c0met0DUTCTF}`

```
C:\Users\Lenovo\Desktop\re1.exe
欢迎来到DUTCTF呦
这是一道很可爱很简单的逆向题呦
输入flag吧:DUTCTF{We1c0met0DUTCTF}
flag get √
请按任意键继续. . .
```