BUUCTF：Mysterious

原创

末 初 于 2020-10-18 16:33:55 发布 1524 收藏 2

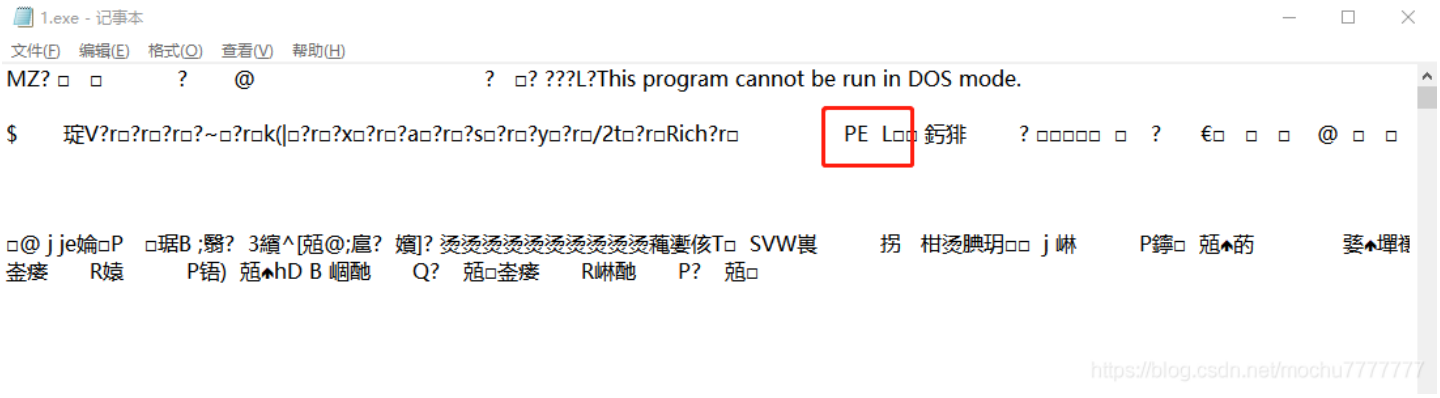
分类专栏： CTF_MISC_Writeup

本文链接：https://blog.csdn.net/mochu7777777/article/details/109146153

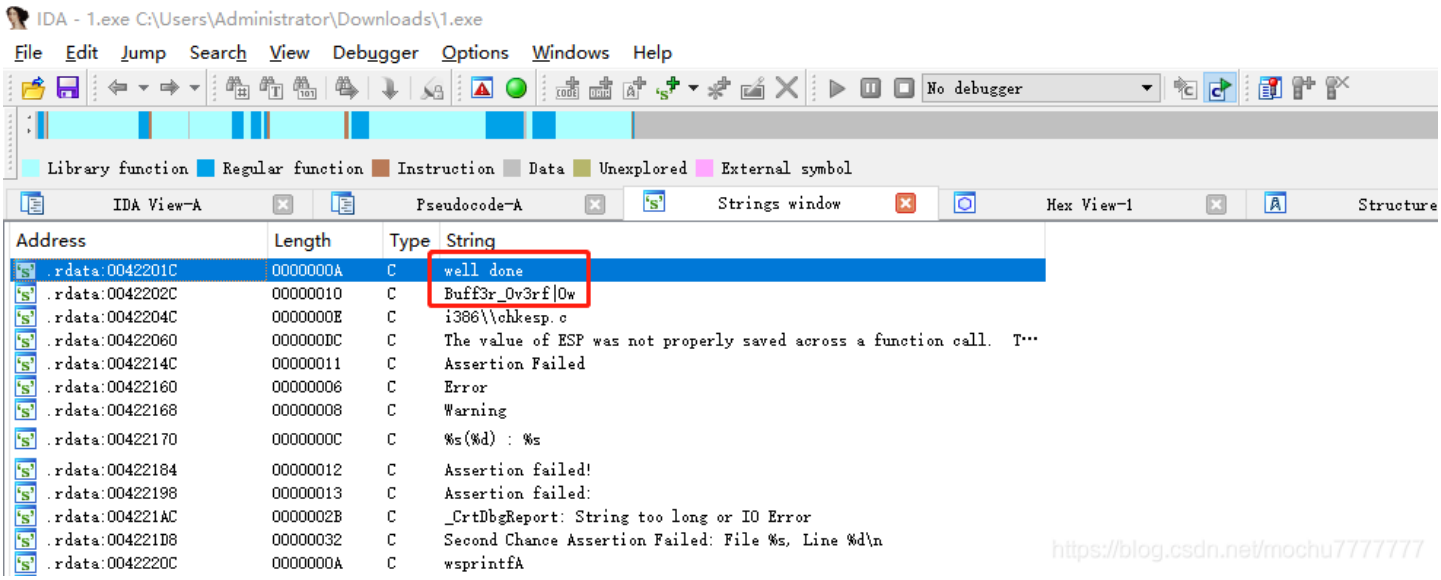
> 题目地址：https://buuoj.cn/challenges#Mysterious

题目附件是一个exe，运行起来让我们输入什么东西，尝试输入了一些字符没有反应

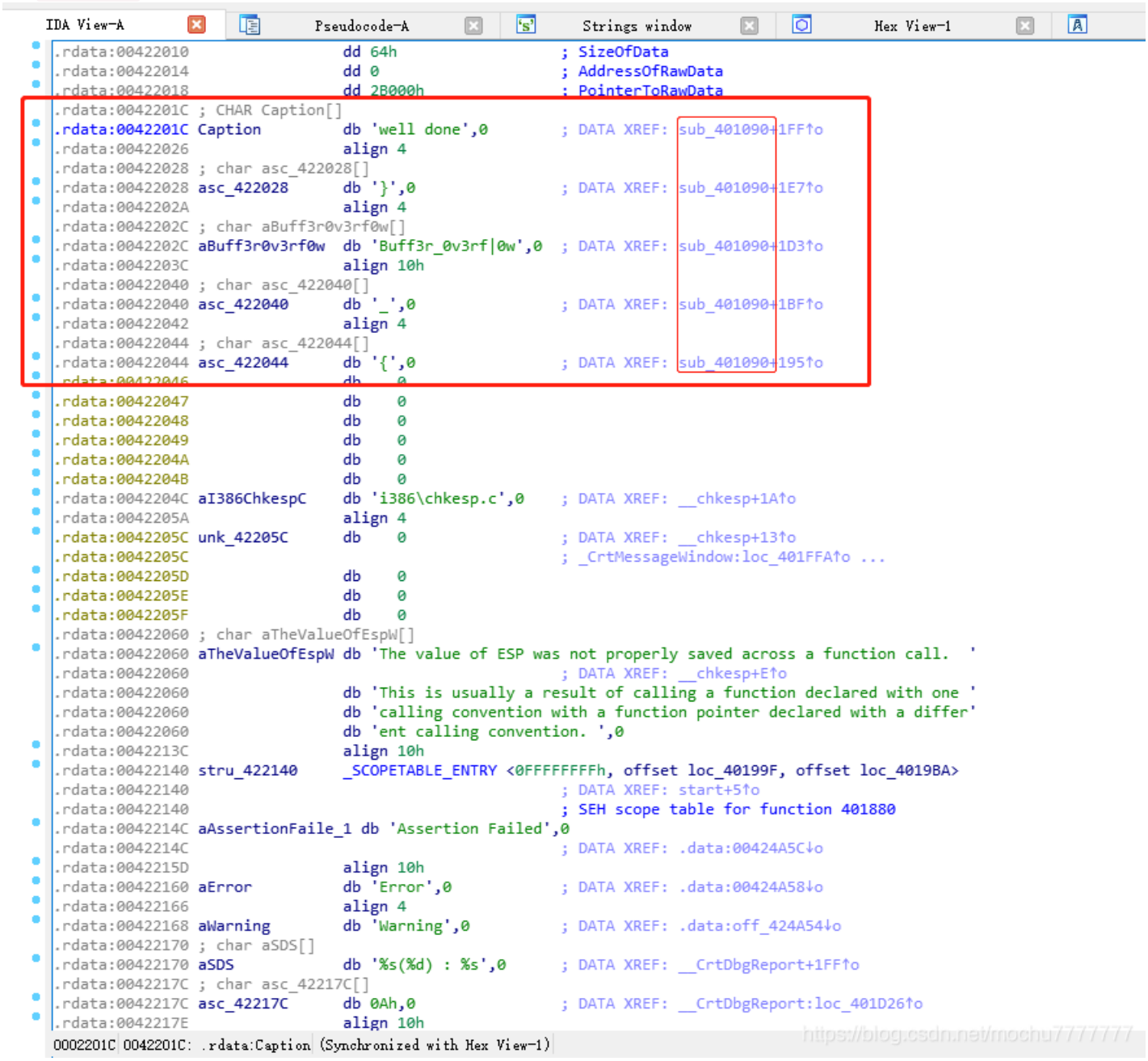
使用记事本打开，查看这个exe是64位的还是32位的



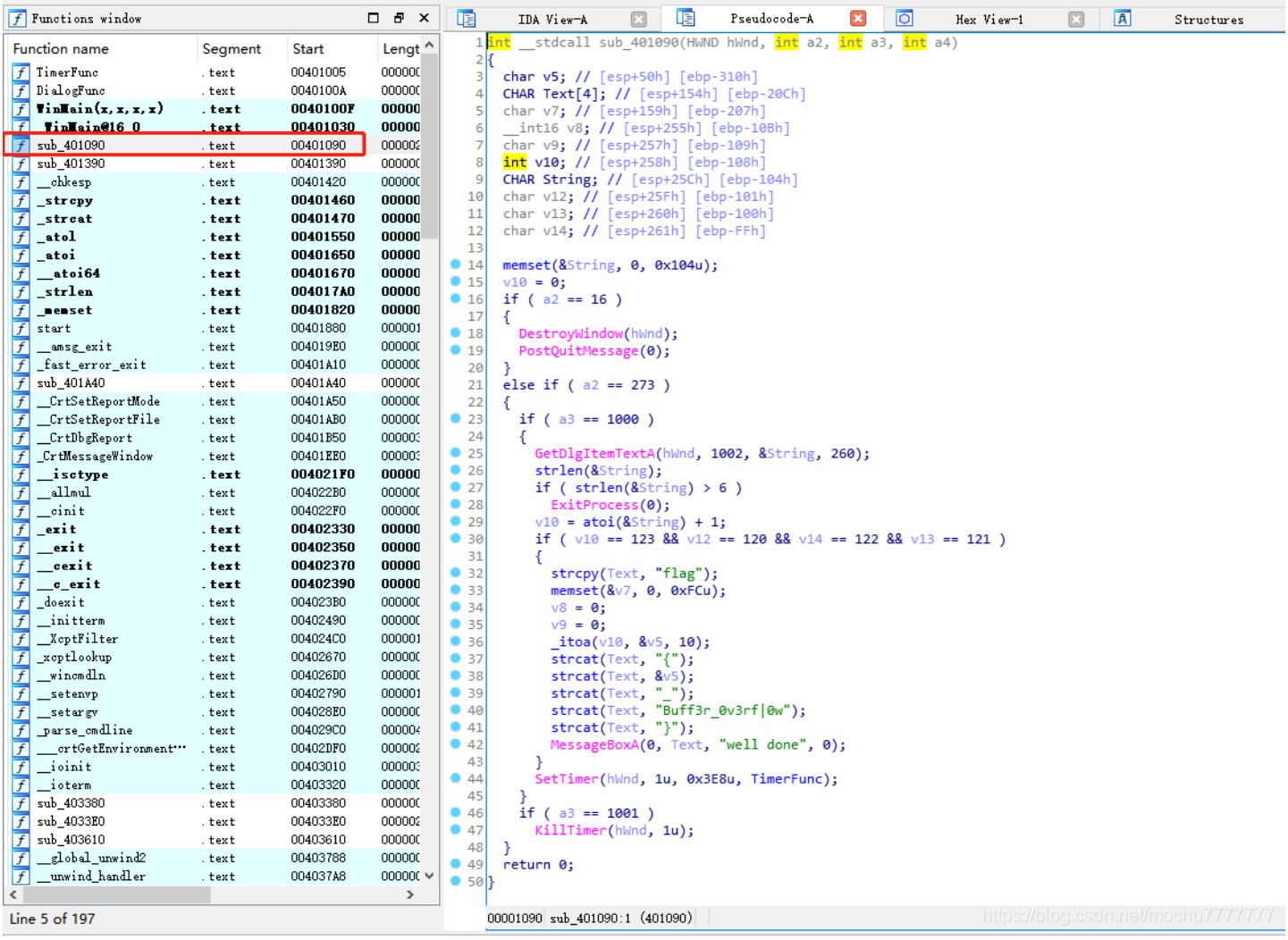
`PE...L...`是32位的exe文件特征，使用ida打开，`Shift+F12`查看字符



点击`well done`，找到了类似flag的字符串



在`Functions Window`找到这个地址，点击，`F5`反汇编查看伪C代码


Functions window
Function name
Segment
Start
Lengt
TimerFunc .text 00401005
DialogFunc .text 0040100A
WinMain(x,x,x,x) .text 0040100F
_WinMain@16 0 .text 00401030
sub_401090 .text 00401090
sub_401390 .text 00401390
__chkesp .text 00401420
_strcpy .text 00401460
_strcat .text 00401470
_atol .text 00401550
_atoi .text 00401650
__atoi64 .text 00401670
_strlen .text 004017A0
_memset .text 00401820
start .text 00401880
__amsg_exit .text 004019E0
_fast_error_exit .text 00401A10
sub_401A40 .text 00401A40
__CrtSetReportMode .text 00401A50
__CrtSetReportFile .text 00401AB0
__CrtDbgReport .text 00401B50
_CrtMessageWindow .text 00401EE0
__isctype .text 004021F0
__allmul .text 004022B0
__cinit .text 004022F0
_exit .text 00402330
__exit .text 00402350
__cexit .text 00402370
__c_exit .text 00402390
_doexit .text 004023B0
__initterm .text 00402490
__XcptFilter .text 004024C0
_xcptlookup .text 00402670
__wincmdln .text 004026D0
__setenvp .text 00402790
__setargv .text 004028E0
_parse_cmdline .text 004029C0
___crtGetEnvironment... .text 00402DF0
__ioinit .text 00403010
__ioterm .text 00403320
sub_403380 .text 00403380
sub_4033E0 .text 004033E0
sub_403610 .text 00403610
__global_unwind2 .text 00403788
__unwind_handler .text 004037A8
Line 5 of 197
IDA View-A
Pseudocode-A
Hex View-1
Structures
1 int __stdcall sub_401090(HWND hWnd, int a2, int a3, int a4)
2 {
3 char v5; // [esp+50h] [ebp-310h]
4 CHAR Text[4]; // [esp+154h] [ebp-20Ch]
5 char v7; // [esp+159h] [ebp-207h]
6 __int16 v8; // [esp+255h] [ebp-10Bh]
7 char v9; // [esp+257h] [ebp-109h]
8 int v10; // [esp+258h] [ebp-108h]
9 CHAR String; // [esp+25Ch] [ebp-104h]
10 char v12; // [esp+25Fh] [ebp-101h]
11 char v13; // [esp+260h] [ebp-100h]
12 char v14; // [esp+261h] [ebp-FFh]
13
14 memset(&String, 0, 0x104u);
15 v10 = 0;
16 if (a2 == 16)
17 {
18 DestroyWindow(hWnd);
19 PostQuitMessage(0);
20 }
21 else if (a2 == 273)
22 {
23 if (a3 == 1000)
24 {
25 GetDlgItemTextA(hWnd, 1002, &String, 260);
26 strlen(&String);
27 if (strlen(&String) > 6)
28 ExitProcess(0);
29 v10 = atoi(&String) + 1;
30 if (v10 == 123 && v12 == 120 && v14 == 122 && v13 == 121)
31 {
32 strcpy(Text, "flag");
33 memset(&v7, 0, 0xFCu);
34 v8 = 0;
35 v9 = 0;
36 _itoa(v10, &v5, 10);
37 strcat(Text, "{");
38 strcat(Text, &v5);
39 strcat(Text, "_");
40 strcat(Text, "Buff3r_0v3rf|0w");
41 strcat(Text, "}");
42 MessageBoxA(0, Text, "well done", 0);
43 }
44 SetTimer(hWnd, 1u, 0x3E8u, TimerFunc);
45 }
46 if (a3 == 1001)
47 KillTimer(hWnd, 1u);
48 }
49 return 0;
50 }
00001090 sub_401090:1 (401090)
https://blog.csdn.net/mochu7777777

```
int __stdcall sub_401090(HWND hWnd, int a2, int a3, int a4)
{
  char v5; // [esp+50h] [ebp-310h]
  CHAR Text[4]; // [esp+154h] [ebp-20Ch]
  char v7; // [esp+159h] [ebp-207h]
  __int16 v8; // [esp+255h] [ebp-10Bh]
  char v9; // [esp+257h] [ebp-109h]
  int v10; // [esp+258h] [ebp-108h]
  CHAR String; // [esp+25Ch] [ebp-104h]
  char v12; // [esp+25Fh] [ebp-101h]
  char v13; // [esp+260h] [ebp-100h]
  char v14; // [esp+261h] [ebp-FFh]

  memset(&String, 0, 0x104u);
  v10 = 0;
  if ( a2 == 16 )
  {
    DestroyWindow(hWnd);
    PostQuitMessage(0);
  }
  else if ( a2 == 273 )
  {
    if ( a3 == 1000 )
    {
      GetDlgItemTextA(hWnd, 1002, &String, 260);
      strlen(&String);
      if ( strlen(&String) > 6 )
        ExitProcess(0);
      v10 = atoi(&String) + 1;
      if ( v10 == 123 && v12 == 120 && v14 == 122 && v13 == 121 )
      {
        strcpy(Text, "flag");
        memset(&v7, 0, 0xFCu);
        v8 = 0;
        v9 = 0;
        _itoa(v10, &v5, 10);
        strcat(Text, "{");
        strcat(Text, &v5);
        strcat(Text, "_");
        strcat(Text, "Buff3r_0v3rf|0w");
        strcat(Text, "}");
        MessageBoxA(0, Text, "well done", 0);
      }
      SetTimer(hWnd, 1u, 0x3E8u, TimerFunc);
    }
    if ( a3 == 1001 )
      KillTimer(hWnd, 1u);
  }
  return 0;
}
```

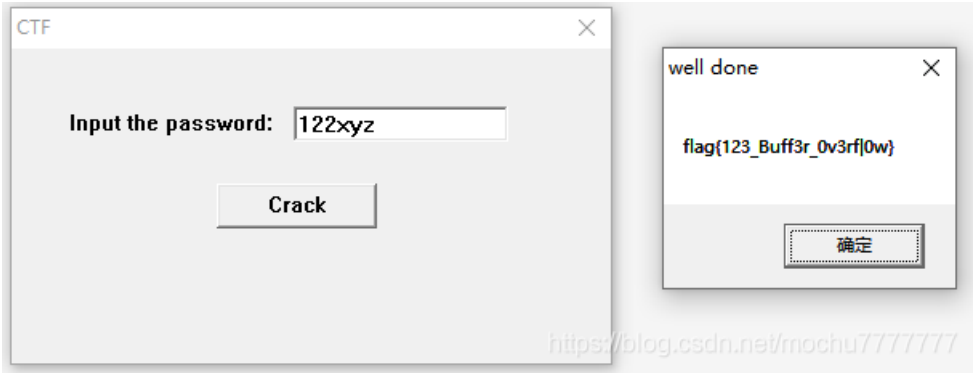
满足

```
if ( v10 == 123 && v12 == 120 && v14 == 122 && v13 == 121 )
```

输入的字符长度不能大于`6`，否则结束程序，`v10`被`atoi()`函数转为数字整型并且`+1`，那么满足条件的`v10`应该为`122`，`v12`、`v13`、`v14`对应的Ascii字符为`xyz`，所以输入

```
122xyz
```

即可得到flag



从伪C代码里面按照程序拼接也可以得到flag

```
flag{123_Buff3r_0v3rf|0w}
```