XCTF Mysterious

原创

酸酸菜鱼 于 2020-07-19 23:51:39 发布 207 收藏
分类专栏： CTF

```
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 == 0x111 )
  {
    if ( a3 == 1000 )
    {
      GetDlgItemTextA(hWnd, 1002, &String, 260);
      strlen(&String);
      if ( strlen(&String) > 6 )
        ExitProcess(0);
      v10 = atoi(&String) + 1;                    //"{"的int值为123，所以string为122
      if ( v10 == '{' && v12 == 'x' && v14 == 'z' && v13 == 'y' )  //输入的值要是这个，而不是flag。所以是 122xy
      {
        strcpy(Text, "flag");
        memset(&v7, 0, 0xFCu);
        v8 = 0;
        v9 = 0;
        _itoa(v10, &v5, 10);
        strcat(Text, "{");
        strcat(Text, &v5);                        // 此处就是整数转字符串，但内容看起来是一样的 123转‘123’,耗费相当
        strcat(Text, "_");
        strcat(Text, "Buff3r_0v3rf|0w");          // flag{123_Buff3r_0v3rf|0w}
        strcat(Text, "}");
        MessageBoxA(0, Text, "well done", 0);
      }
      SetTimer(hWnd, 1u, 0x3E8u, TimerFunc);
    }
    if ( a3 == 1001 )
      KillTimer(hWnd, 1u);
  }
  return 0;
}
```

受惯性思维影响。以为要输入flag才行，忽略了逻辑。

1.输入：122xyz 会弹出flag

2.修改汇编代码，执行弹窗，出flag