攻防世界 Mysterious wp

原创

__ys 于 2020-12-07 17:41:15 发布 148 收藏

分类专栏： RE # 攻防世界

本文链接：https://blog.csdn.net/qq_39214793/article/details/110823224

RE 同时被 2 个专栏收录

35 篇文章 0 订阅

订阅专栏

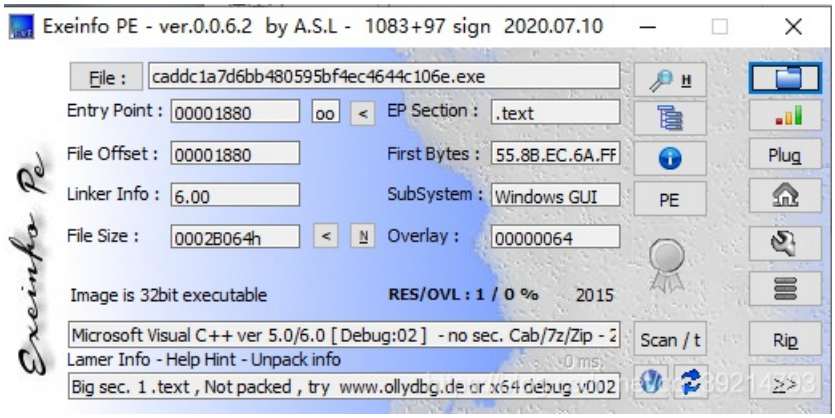
攻防世界

25 篇文章 0 订阅

订阅专栏

攻防世界 Mysterious

1. exeinfope查壳



发现无壳

2. 载入IDA，进入主函数

```
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 == 'x' && v14 == 'z' && v13 == 'y' )
      {
        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;
}
```


里面有一些没见过的函数，~~通过百度~~

> atoi 是把字符串转换成整型数的一个函数。
> int atoi(const char *nptr) 函数会扫描参数 nptr字符串，会跳过前面的空白字符（例如空格，tab缩进）等。如果 nptr不能转换成 int 或者 nptr为空字符串，那么将返回 0 。
> **特别注意，该函数要求被转换的字符串是按十进制数理解的。atoi输入的字符串对应数字存在大小限制（与int类型大小有关），若其过大可能报错-1。**

> _itoa是将整形转换为字符串
> char_itoa(int value,char* string,int radix);
> 参数说明
> value-----要转换的整形值
> string-----转换后的字符串
> radix------表示基数(2, 8, 10, 16)等进制基数

知道这两个函数的含义后题目就很明了了

```
GetDlgItemTextA(hWnd, 1002, &String, 260);
strlen(&String);
if ( strlen(&String) > 6 )
  ExitProcess(0);
```

此处是输入，且输入长度不大于6

```
v10 = atoi(&String) + 1;
if ( v10 == 123 && v12 == 'x' && v14 == 'z' && v13 == 'y' )
{
  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);
```


由此处可知当v10=123（输入即为122），v5=123。
目前我们就可以知晓flag为

> flag{123_Buff3r_0v3rf|0w}

我们也可以在输入框中输入122xyz直接得到flag