攻防世界 Reverse高手进阶区 2分题 Mysterious

原创

思源湖的鱼 于 2020-12-02 13:50:22 发布 167 收藏

分类专栏： ctf 文章标签： ctf 攻防世界 reverse

本文链接：https://blog.csdn.net/weixin_44604541/article/details/110479100

前言

继续ctf的旅程

攻防世界Reverse高手进阶区的2分题

本篇是Mysterious的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

得到一个exe

PE查壳

扔进IDA

```
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 }
```


可以看到只要求v5即可

跟踪`_itoa`函数

```
char *__cdecl _itoa(int a1, char *a2, int a3)
{
  if ( a3 != 10 || a1 >= 0 )
    xtoa(a1, a2, a3, 0);
  else
    xtoa(a1, a2, 10, 1);
  return a2;
}
```

```
int __cdecl xtoa(unsigned int a1, char *a2, unsigned int a3, int a4)
{
  char v4; // ST00_1
  int result; // eax
  unsigned int v6; // [esp+4h] [ebp-Ch]
  char *v7; // [esp+8h] [ebp-8h]
  char *v8; // [esp+Ch] [ebp-4h]
  char *v9; // [esp+Ch] [ebp-4h]

  v8 = a2;
  if ( a4 )
  {
    *a2 = 45;
    v8 = a2 + 1;
    a1 = -a1;
  }
  v7 = v8;
  do
  {
    v6 = a1 % a3;
    a1 /= a3;
    if ( v6 <= 9 )
      *v8 = v6 + 48;
    else
      *v8 = v6 + 87;
    ++v8;
  }
  while ( a1 );
  *v8 = 0;
  v9 = v8 - 1;
  do
  {
    v4 = *v9;
    *v9 = *v7;
    *v7 = v4;
    --v9;
    result = (int)(v7++ + 1);
  }
  while ( v7 < v9 );
  return result;
}
```


发现`_itoa`函数的作用就是将整形转为字符型

所以v5的值为`123`

得到`flag{123_Buff3r_0v3rf|0w}`

结语

简单题