攻防世界 Reverse高手进阶区 2分题 srm-50

原创

思源湖的鱼 于 2020-12-01 14:11:02 发布 118 收藏

分类专栏： ctf 文章标签： 攻防世界 ctf reverse

本文链接：https://blog.csdn.net/weixin_44604541/article/details/110430420

前言

继续ctf的旅程

攻防世界Reverse高手进阶区的2分题

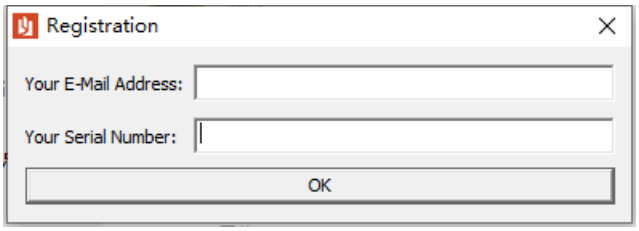
本篇是srm-50的writeup

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

下下来一个exe



PE查壳

扔进IDA

```
BOOL __stdcall DialogFunc(HWND hDlg, UINT a2, WPARAM a3, LPARAM a4)
{
  HMODULE v5; // eax
  HICON v6; // eax
  HMODULE v7; // eax
  HCURSOR v8; // ST20_4
  HWND v9; // eax
  CHAR String; // [esp+8h] [ebp-340h]
  CHAR v11[4]; // [esp+108h] [ebp-240h]
  char v12; // [esp+10Ch] [ebp-23Ch]
  char v13; // [esp+10Dh] [ebp-23Bh]
  char v14; // [esp+10Eh] [ebp-23Ah]
  char v15; // [esp+10Fh] [ebp-239h]
  char v16; // [esp+110h] [ebp-238h]
  char v17; // [esp+111h] [ebp-237h]
  char v18; // [esp+112h] [ebp-236h]
  char v19; // [esp+113h] [ebp-235h]
  char v20; // [esp+114h] [ebp-234h]
  char v21; // [esp+115h] [ebp-233h]
  char v22; // [esp+116h] [ebp-232h]
  char v23; // [esp+117h] [ebp-231h]
  CHAR Text; // [esp+208h] [ebp-140h]
  char Src[16]; // [esp+308h] [ebp-40h]
  __int128 v26; // [esp+318h] [ebp-30h]
  int v27; // [esp+328h] [ebp-20h]
  __int128 v28; // [esp+32Ch] [ebp-1Ch]
  int v29; // [esp+33Ch] [ebp-Ch]
  __int16 v30; // [esp+340h] [ebp-8h]
```

```
30  if ( a2 == 16 )
31  {
32    EndDialog(hDlg, 0);
33    return 0;
34  }
35  if ( a2 == 272 )
36  {
37    v5 = GetModuleHandleW(0);
38    v6 = LoadIconW(v5, (LPCWSTR)0x67);
39    SetClassLongA(hDlg, -14, (LONG)v6);
40    v7 = GetModuleHandleW(0);
41    v8 = LoadCursorW(v7, (LPCWSTR)0x66);
42    v9 = GetDlgItem(hDlg, 1);
43    SetClassLongA(v9, -12, (LONG)v8);
44    return 1;
45  }
46  if ( a2 != 273 || (unsigned __int16)a3 != 1 )
47    return 0;
48  memset(&String, (unsigned __int16)a3 - 1, 0x100u);
49  memset(v11, 0, 0x100u);
50  memset(&Text, 0, 0x100u);
51  GetDlgItemTextA(hDlg, 1001, &String, 256);
52  GetDlgItemTextA(hDlg, 1002, v11, 256);
53  if ( strstr(&String, "@") && strstr(&String, ".") && strstr(&String, ".")[1] && strstr(&String, "@")[1] != 46 )
54  {
55    v28 = xmmword_410AA0;
56    v29 = 1701999980;
57    *(_OWORD *)Src = xmmword_410A90;
58    v30 = 46;
59    v26 = xmmword_410A80;
60    v27 = 3830633;
```



```
61    if ( strlen(v11) != 16
62      || v11[0] != 67
63      || v23 != 88
64      || v11[1] != 90
65      || v11[1] + v22 != 155
66      || v11[2] != 57
67      || v11[2] + v21 != 155
68      || v11[3] != 100
69      || v20 != 55
70      || v12 != 109
71      || v19 != 71
72      || v13 != 113
73      || v13 + v18 != 170
74      || v14 != 52
75      || v17 != 103
76      || v15 != 99
77      || v16 != 56 )
78    {
79      strcpy_s(&Text, 0x100u, (const char *)&v28);
80    }
81    else
82    {
83      strcpy_s(&Text, 0x100u, Src);
84      strcat_s(&Text, 0x100u, v11);
85    }
86  }
87  else
88  {
89    strcpy_s(&Text, 0x100u, "Your E-mail address in not valid.");
90  }
91  MessageBoxA(hDlg, &Text, "Registeration", 0x40u);
92  return 1;
93}
```


关键的if判断如下

```
if (strlen(v12) != 16                //序列号长度要等于16
            || v12[0] != 67          //第一个字符要为字母C
            || v24 != 88             //v24要为字母X
            || v12[1] != 90          //第二个字符要为字母Z
            || v12[1] + v23 != 155   //v23要为字母A
            || v12[2] != 57          //第三个字符要为数字9
            || v12[2] + v22 != 155   //v22要为字母b
            || v12[3] != 100         //第四个字符要为字母d
            || v21 != 55             //v21要为数字7
            || v13 != 109            //v13要为字母m
            || v20 != 71             //v20要为字母G
            || v14 != 113            //v14要为字母q
            || v14 + v19 != 170      //v19要为数字9
            || v15 != 52             //v15要为数字4
            || v18 != 103            //v18要为字母g
            || v16 != 99             //v16要为字母c
            || v17 != 56)            //v17要为字母8
```

又esp+108是V12[0]，esp+109是v12[1]，esp+10A是v12[2]，esp+10B是v12[3]，esp+10C是v13…，按照这个存储顺序，依次类推就能得出flag：`CZ9dmq4c8g9G7bAX`

结语

简单题