


攻防世界 逆向 Mysterious

原创

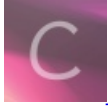
[与日平肩以头抢地](#)  于 2020-03-01 17:06:48 发布  747  收藏 1

分类专栏: [逆向](#) 文章标签: [安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/fool_best/article/details/104594939

版权



[逆向](#) 专栏收录该内容

12 篇文章 0 订阅

订阅专栏

攻防世界 逆向 Mysterious

(原创)

原题如下:

Mysterious

最佳Writeup由admin提供

WP 建议

难度系数: ★ 1.0

题目来源: BUUCTF-2019

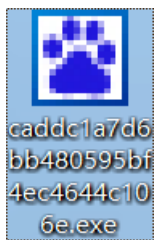
题目描述: 自从报名了CTF竞赛后,小明就辗转于各大论坛,但是对于逆向题目仍是一知半解。有一天,一个论坛老鸟给小明发了一个神秘的盒子,里面有开启逆向思维的秘密。小明如获至宝,三天三夜,终于解答出来了,聪明的你能搞定这个神秘盒子么? (答案为flag{XXX}形式)

题目场景: 暂无

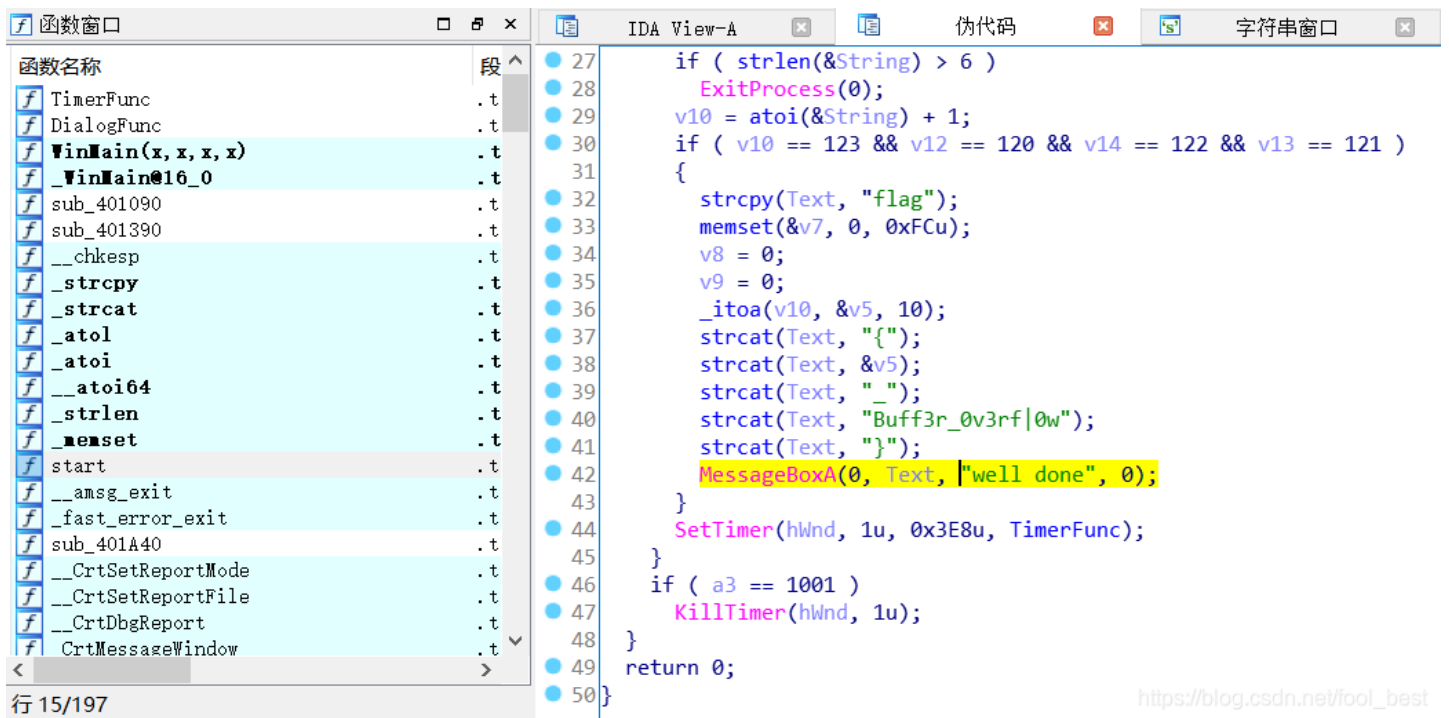
题目附件: 附件1

https://blog.csdn.net/fool_best

下载文件:



用IDA打开,找到start函数,进行反编译



```
函数窗口 | IDA View-A | 伪代码 | 字符串窗口
函数名称 | 段 | 行号 | 代码
TimerFunc | .t | 27 | if ( strlen(&String) > 6 )
DialogFunc | .t | 28 |     ExitProcess(0);
WinMain(x, x, x) | .t | 29 | v10 = atoi(&String) + 1;
_WinMain@16_0 | .t | 30 | if ( v10 == 123 && v12 == 120 && v14 == 122 && v13 == 121 )
sub_401090 | .t | 31 | {
sub_401390 | .t | 32 |     strcpy(Text, "flag");
sub_401390 | .t | 33 |     memset(&v7, 0, 0xFCu);
__chkesp | .t | 34 |     v8 = 0;
_strcpy | .t | 35 |     v9 = 0;
_strcat | .t | 36 |     _itoa(v10, &v5, 10);
_atol | .t | 37 |     strcat(Text, "{");
_atoi | .t | 38 |     strcat(Text, &v5);
_atoi64 | .t | 39 |     strcat(Text, "_");
_strlen | .t | 40 |     strcat(Text, "Buff3r_0v3rf|0w");
memset | .t | 41 |     strcat(Text, "}");
start | .t | 42 |     MessageBoxA(0, Text, "well done", 0);
__amsg_exit | .t | 43 | }
_fast_error_exit | .t | 44 |     SetTimer(hWnd, 1u, 0x3E8u, TimerFunc);
sub_401A40 | .t | 45 | }
__CrtSetReportMode | .t | 46 | if ( a3 == 1001 )
__CrtSetReportFile | .t | 47 |     KillTimer(hWnd, 1u);
__CrtDbgReport | .t | 48 | }
CrtMessageWindow | .t | 49 | return 0;
| | | 50 | }
```

行 15/197

https://blog.csdn.net/fool_best

源代码如下:

```

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;
}

```

flag在这个地方:

```
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);
}
```

可以知道v10=123, 要求得v5。打开_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, 0xAu, 1);
    return a2;
}
```

根据条件if成立, 打开xtoa函数 (a1=123,a3=10)。

xtoa的关键代码是

```

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;

```

`_itoa`函数的作用就是将整形转为字符型。

求得v5的值为123。

得到flag{123_Buff3r_0v3rf0w}