

2019安恒萌新粉丝有奖答题CTF逆向题Mysterious题目 Writeup

原创

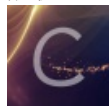
iqiqiya 于 2019-03-28 21:21:58 发布 3335 收藏 1

分类专栏: [我的逆向之路](#) [我的CTF之路](#) [-----安恒CTF](#) [我的CTF进阶之路](#) 文章标签: [Mysterious CTF逆向题](#) [2019安恒萌新粉丝有奖答题](#) [Writeup](#)

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/xiangshangbashaonian/article/details/88878576>

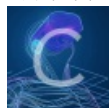
版权



[我的逆向之路](#) 同时被 3 个专栏收录

108 篇文章 10 订阅

订阅专栏



[我的CTF之路](#)

92 篇文章 5 订阅

订阅专栏



[-----安恒CTF](#)

6 篇文章 1 订阅

订阅专栏

题目信息:

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{}形式, 提交{}内内容即可)

解题思路:

这道题目通过字符串可以确定关键代码

稍做分析可以确定主要是利用了atoi()函数的特性

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。

那我们只需要动态调试几次就可以分析出来

ction Regular function Instruction Data Unexplored External symbol

indow IDA View-A Strings window Hex View-1 Structures

Address	Length	Type	String
.rdata:0...	0000000A	C	well done
.rdata:0...	00000010	C	Buff3r_0v3rf 0w
.rdata:0...	0000000E	C	i386\\chkesp.c
.rdata:0...	000000DC	C	The value of ESP was not properly saved across a function cal...
.rdata:0...	00000011	C	Assertion Failed
.rdata:0...	00000006	C	Error
.rdata:0...	00000008	C	Warning
.rdata:0...	0000000C	C	%s(%d) : %s
.rdata:0...	00000012	C	Assertion failed!
.rdata:0...	00000013	C	Assertion failed:

<https://blog.csdn.net/xiangshangbashaonian>

```

.t 23 if ( a3 == 1000 )
.t 24 {
.t 25 GetDlgItemTextA(hWnd, 1002, &String, 260); // 获取我们的输入
.t 26 strlen(&String); // 计算长度
.t 27 if ( strlen(&String) > 6 ) // 长度必须满足小于等于6
.t 28 ExitProcess(0);
.t 29 v10 = atoi(&String) + 1; // atoi()函数将字符串转换成整型并+1
.t 30 if ( v10 == 123 && v12 == 'x' && v14 == 'z' && v13 == 'y' )
.t 31 {
.t 32 strcpy(Text, "flag");
.t 33 memset(&v7, 0, 0xFCu);
.t 34 v8 = 0;
.t 35 v9 = 0;
.t 36 _itoa(v10, &v5, 10); // 用itoa()将整型转回字符串
.t 37 strcat(Text, "{");
.t 38 strcat(Text, &v5);
.t 39 strcat(Text, "_");
.t 40 strcat(Text, "Buff3r_0v3rf|0w");
.t 41 strcat(Text, "}");
.t 42 MessageBoxA(0, Text, "well done", 0);
.t 43 }
.t 44 SetTimer(hWnd, 1u, 0x3E8u, TimerFunc);

```

<https://blog.csdn.net/xiangshangbashaonian>

```

debug007:0019F6DC db 7Bh ; {
debug007:0019F6DD db 79h ; y
debug007:0019F6DE db 78h ; x
debug007:0019F6DF db 7Ah ; z
debug007:0019F6E0 db 32h ; 2
debug007:0019F6E1 db 30h ; 0
debug007:0019F6E2 db 35h ; 5
debug007:0019F6E3 db 34h ; 4 ; var101
debug007:0019F6E4 db 37h ; 7 ; var100
debug007:0019F6E5 db 31h ; 1 ; varFF
debug007:0019F6E6 db 35h ; 5
debug007:0019F6E7 db 37h ; 7
debug007:0019F6E8 db 37h ; 7
debug007:0019F6E9 db 30h ; 0

```

<https://blog.csdn.net/xiangshangbashaonian>

```

.text:004011B4 movsx eax, [ebp+var_101] ; E3
.text:004011BB cmp eax, 'x'
.text:004011BE jnz loc_4012AA
.text:004011C4 movsx ecx, [ebp+var_FF] ; E4
.text:004011CB cmp ecx, 'z'
.text:004011CE jnz loc_4012AA
.text:004011D4 movsx edx, [ebp+var_100] ; E5
.text:004011DB cmp edx, 'y'
.text:004011DE jnz loc_4012AA

```

可以判断出来输入恰好六位 后三位很容易确定为xyz

前三位的话是十进制的“{” 也就是123 记得减1 也就是122

最后确定为122xyz

