

实验吧CTFreverse题目证明自己吧writeup

原创

iqiqiya 于 2018-09-11 19:57:40 发布 1161 收藏 2

分类专栏: [我的逆向之路](#) [我的CTF之路](#) -----[实验吧CTF](#) [我的CTF进阶之路](#) 文章标签: [实验吧CTFreverse题目证明自己吧题解](#) [证明自己吧](#) [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/82631654>

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



[-----实验吧CTF](#)

6 篇文章 0 订阅

订阅专栏

题目地址: <http://ctf5.shiyanbar.com/crackme/>

先运行下

```
Can you Guess the Code: 111111111
https://blog.csdn.net/xiangshangbashaonian
```

发现输入错误就会闪退

没有加壳

载入IDA 搜索字符串

t	[s]	.rdata:0...	0000000C	C	MessageBoxA
t	[s]	.rdata:0...	0000000B	C	user32.dll
t	[s]	.rdata:0...	0000000D	C	KERNEL32.dll
t	[s]	.data:00...	00000015	C	You Don't Guess it~\n
t	[s]	.data:00...	00000025	C	Good! The Key is your input o(^o^o)\n
t	[s]	.data:00...	00000019	C	Can you Guess the Code:
t	[s]	.data:00...	00000006	C	粒冢
t	[s]	.data:00...	00000006	C	粒冢
t	[s]	.data:00...	00000006	C	粒冢
t	[s]	.data:00...	00000006	C	粒冢

```

| .data:00407045          align 4
| .data:00407048 aGoodTheKeyIsYo db 'Good! The Key is your input o(^o^)',0Ah,0
| .data:00407048          ; DATA XREF: _main+7810
| .data:0040706D          align 10h
| .data:00407070 aCanYouGuessThe db 'Can you Guess the Code: ',0
| .data:00407070          ; DATA XREF: _main+6f0
| .data:00407089          align 4
| .data:0040708C dword_40708C dd 48195768h ; DATA XREF: sub_401060+3tr
| .data:00407090 dword_407090 dd 78586E50h ; DATA XREF: sub_401060+81tr
| .data:00407094 dword_407094 dd 59106A54h ; DATA XREF: sub_401060+20tr

```

```

1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     int v4; // [esp+0h] [ebp-7D0h]
4
5     sub_4011BA(aCanYouGuessThe, v4);
6     gets(&v4); // 获得输入
7     if ( sub_401060(&v4) ) // 我们的input经过函数sub_401060()的处理返回值为1 那就正确
8         sub_4011BA(aGoodTheKeyIsYo, v4);
9     else
10        sub_4011BA(aYouDontGuessIt, v4);
11    return 0;
12}

```

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

```

signed int __cdecl sub_401060(const char *input)
{
    unsigned int i; // edx
    unsigned int j; // edx
    int v3; // edx
    int v5; // [esp+Ch] [ebp-10h]
    int v6; // [esp+10h] [ebp-Ch]
    int v7; // [esp+14h] [ebp-8h]
    __int16 v8; // [esp+18h] [ebp-4h]
    char v9; // [esp+1Ah] [ebp-2h]

    v5 = dword_40708C;
    v6 = dword_407090;
    v8 = word_407098;
    v9 = byte_40709A;
    v7 = dword_407094;

    if ( strlen(input) == strlen(&v5) ) // 如果我们输入的长度=v5的长度
    {

```

```

i = 0;

if ( strlen(input) != 0 )                // 如果len(input) != 0 且i<len(input)
{
    do
        input[i++] ^= 0x20u;            // 与0x20u异或
    while ( i < strlen(input) );
}

j = 0;

if ( strlen(&v5) != 0 )                  // 对v5进行-5
{
    do
        *(&v5 + j++) -= 5;
    while ( j < strlen(&v5) );          // 那我们只需要倒过来操作 先-5 再与0x20异或即可得到flag
}

v3 = 0;

if ( strlen(&v5) == 0 )
    return 1;

while ( *(&v5 + v3 + input - &v5) == *(&v5 + v3) )
{
    if ( ++v3 >= strlen(&v5) )
        return 1;
}

return 0;
}

```

```
证明自己吧.py x
1 v5 = [0x68, 0x57, 0x19, 0x48, 0x50, 0x6E, 0x58, 0x78, 0x54, 0x6A,
2     0x19, 0x58, 0x5E, 0x06]
3 flag = ''
4 for i in range(0, len(v5)):
5     v5[i] -= 5
6     v5[i] ^= 0x20
7     flag += chr(v5[i])
8 print(flag)
9

Run: 证明自己吧 x
C:\Users\...PycharmProjects\test\Scripts\python.exe C:/Users/.../PycharmProjects/reverse/实验吧/证明自己吧.py
Cr4ckIsSoE4sy!
Process finished with exit code 0
https://blog.csdn.net/xiangshangbashaonian
```

得到flag: Cr4ckIsSoE4sy!