

实验吧CTFreverse题目该题不简单writeup

原创

iqiqiya 于 2018-09-12 19:08:49 发布 3593 收藏 3

分类专栏: [我的逆向之路](#) -----[实验吧CTF](#) [我的CTF之路](#) [我的CTF进阶之路](#) 文章标签: [实验吧CTF reverse](#) [题目该题不简单](#) [writeup](#) [reverse](#) [该题不简单](#) [writeup](#) [crackme](#)

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/82666631>

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



[-----实验吧CTF](#)

6 篇文章 0 订阅

订阅专栏



[我的CTF之路](#)

92 篇文章 5 订阅

订阅专栏

题目链接:

<http://ctf5.shiyanbar.com/crack/3/>

该题不简单 分值: 50

来源: [西普学院](#)

难度: [难](#)

参与人数: [4918人](#)

Get Flag: [974人](#)

无语了, 想给你们制造点悬念都没有了, 哎! 直接去做题吧

解题链接: <http://ctf5.shiyanbar.com/crack/3/ian> [通过](#) [ingbashaonian](#)

运行 显示密钥无效



查壳无壳

载入IDA

查看字符串

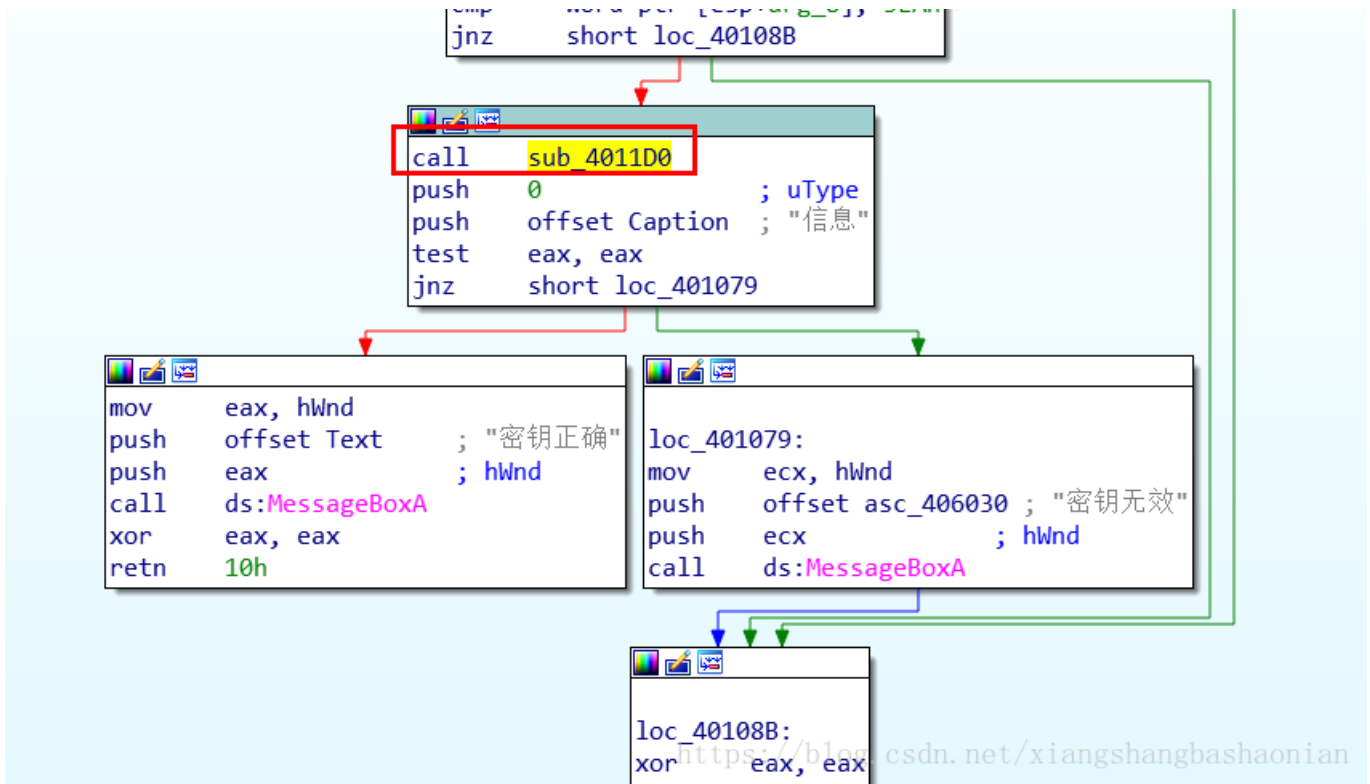
发现密钥正确

双击进入

```

[s] .rdata:0000001A C Runtime Error!\n\nProgram:
[s] .rdata:00000017 C <program name unknown>
[s] .rdata:00000013 C GetLastErrorPopup
[s] .rdata:00000010 C GetActiveWindow
[s] .rdata:0000000C C MessageBoxA
[s] .rdata:0000000B C user32.dll
[s] .rdata:0000000D C KERNEL32.dll
[s] .rdata:0000000B C USER32.dll
[s] .data:00000008 C 密钥无效
[s] .data:00000008 C 密钥正确
[s] .data:00000005 C 信息
[s] .data:00000011 C CrackMe 2011 # 2
[s] .data:00000006 C 粒冢
[s] .data:00000006 C 粒冢
[s] .data:00000006 C ht澧据[//blog.csdn.net/xiangshangbashaonian
[s] .data:00000005 C @~一

```



分析找到关键函数sub_4011D0

F5反汇编成c代码

```

v8 = 0;
if ( GetDlgItemTextA(hDlg, 1000, String, 16) < 5 )
    return 1;
GetDlgItemTextA(hDlg, 1001, &String1, 16);
v1 = 0;
if ( strlen(String) != 0 )
{
    do
    {
        *(&String2 + v1) = (v1 + v1 * String[v1] * String[v1]) % 0x42 + 33;
        ++v1;
    }
    while ( v1 < strlen(String) );
}
strcpy(String, "Happy@");
lstrcatA(String, &String2);
return lstrcmpA(&String1, String) != 0;

```

分析得到关键

Py大法好:

```
该题不简单.py x
1 # -*- coding: utf-8 -*-
2 s = 'Hello'
3 flag = ''
4 for i in range(0, len(s1)):
5     flag += chr((i + i*ord(s1[i])*ord(s1[i])) % 0x42 + 33)
6 print('Happy@'+flag)

Run: 该题不简单 x
C:\Users\11111\PycharmProjects\test\Scripts\python.exe C:/
Happy@!GA0U
https://blog.csdn.net/xiangshangbashaonian
Process finished with exit code 0
```