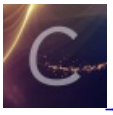
实验吧CTFreverse题目该题不简单writeup

原创

iqiqiya 于 2018-09-12 19:08:49 发布
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


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/

运行 显示密钥无效

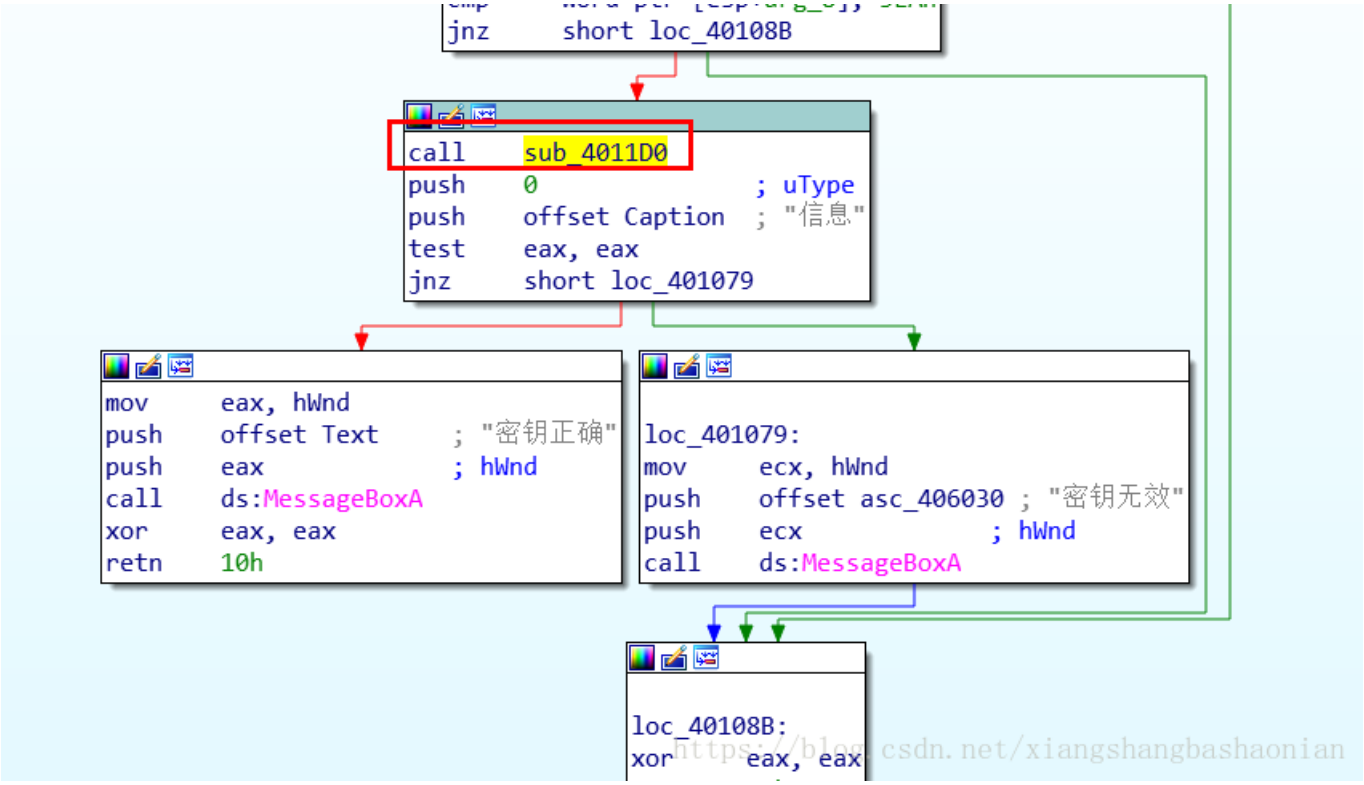
查壳无壳

载入IDA

查看字符串

发现密钥正确

双击进入



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：