看雪.Wifi万能钥匙 2017CTF年中赛---第一题

原创

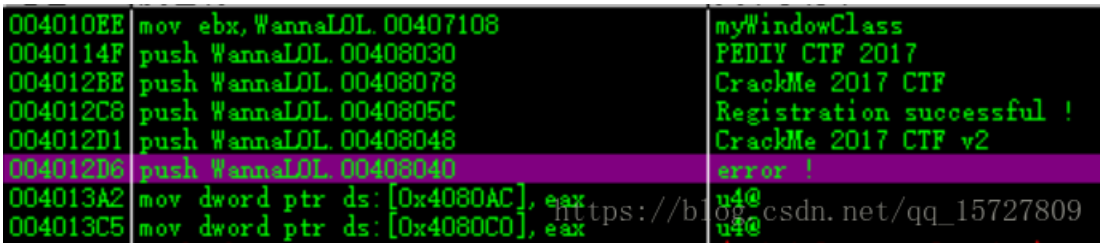
Angelki 于 2018-09-29 10:49:30 发布 504 收藏

分类专栏： CTF 文章标签： CTF

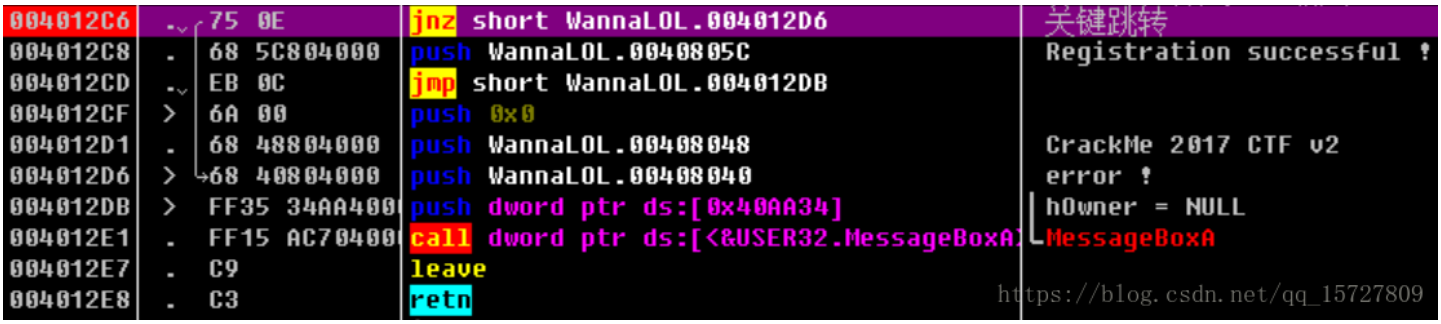
本文链接：https://blog.csdn.net/qq_15727809/article/details/82893603

考察浮点数运算

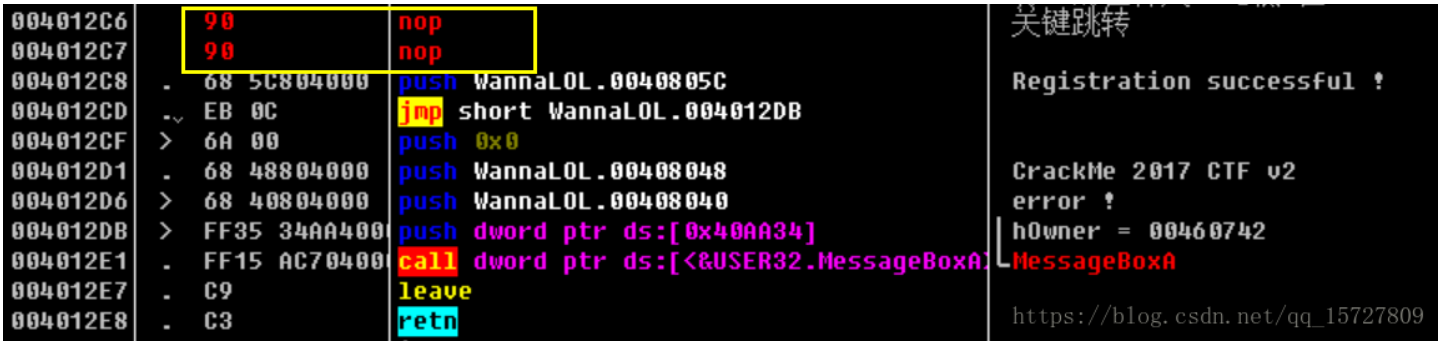
1、OD载入，搜索字符串，查找到错误或正确提示信息，双击点进去。



找到以为的关键跳转，下断点，重新载入，输入注册码，运行，竟然提示错误！



不死心的将关键跳转NOP掉，保存到文件，运行，



结果依然报错！果然爆破不行呀……那就老老实实查看算法吧。

2、在该段开始位置下断点，OD重新载入，运行，输入key，断在段首，仔细分析汇编代码

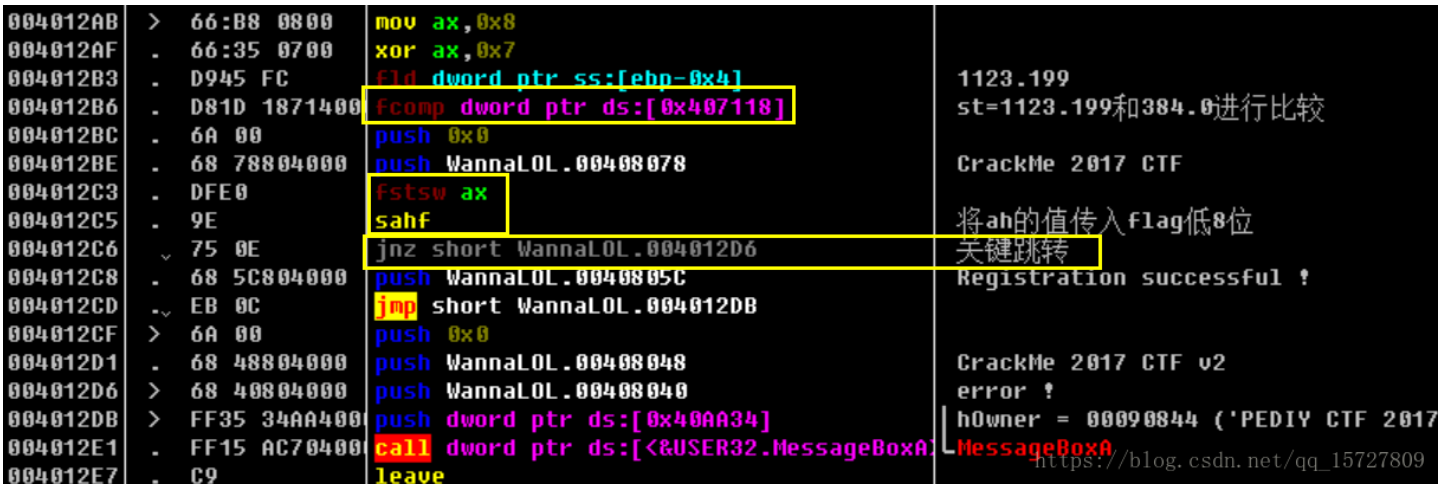
```
0040121C   .  8D45 E4       lea eax,dword ptr ss:[ebp-0x1C]      '123456'
0040121F   .  50            push eax                             '1589'
00401220   .  E8 DB000000   call WannaLOL.00401300
00401225   .  83F8 04       cmp eax,0x4                          eax=6,长度?
00401228   .  59            pop ecx                              将字符串写入ECX
00401229   .v 0F85 A0000000 jnz WannaLOL.004012CF
0040122F   .  6A 30         push 0x30
00401231   .  59            pop ecx                              ECX = 0x30
00401232   .  384D E4       cmp byte ptr ss:[ebp-0x1C],cl        '1'
00401235   .v 0F84 9400000  je WannaLOL.004012CF
0040123B   .  384D E5       cmp byte ptr ss:[ebp-0x1B],cl
0040123E   .v 0F84 8B00000  je WannaLOL.004012CF
00401244   .  384D E6       cmp byte ptr ss:[ebp-0x1A],cl
00401247   .v 0F84 8200000  je WannaLOL.004012CF
0040124D   .  384D E7       cmp byte ptr ss:[ebp-0x19],cl
00401250   .v 74 7D         je short WannaLOL.004012CF
00401252   .  807D E4 31    cmp byte ptr ss:[ebp-0x1C],0x31
00401256   .v 75 77         jnz short WannaLOL.004012CF
00401258   .  807D E5 35    cmp byte ptr ss:[ebp-0x1B],0x35
0040125C   .v 75 71         jnz short WannaLOL.004012CF
0040125E   .v 74 03         je short WannaLOL.00401263
00401260   .v 75 01         jnz short WannaLOL.00401263
```


发现程序，首先判断输入长度是否等于4，如果不是则直接报错；接着将4个字符分别存入[ebp-0x1C]、[ebp-0x1B]、[ebp-0x1A]、[ebp-0x19]；然后将第1个字符与“1”比较，第2个字符与“5”比较，如果不等则报错。
也即key的前2个字符是15

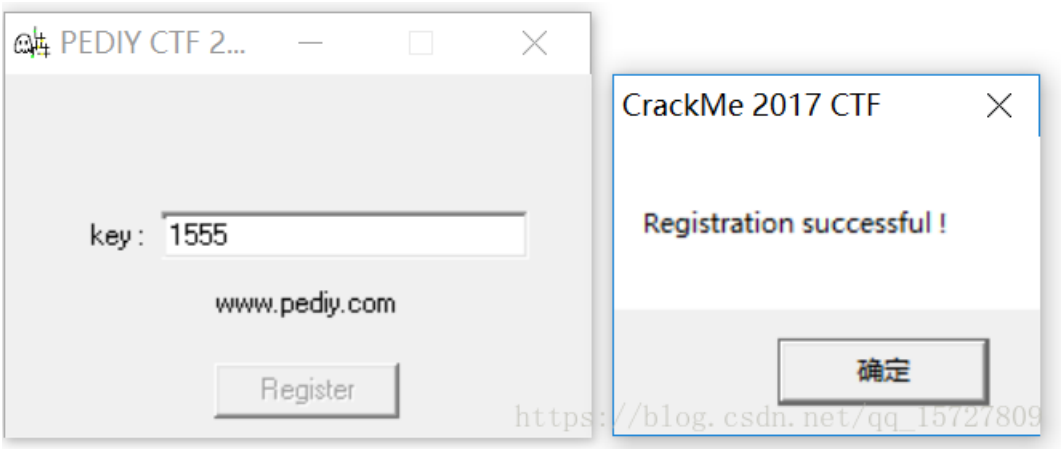
3、继续向下分析，这次我输入的是“1589”

发现流程是这样的：首先把1和5转为浮点数1.0和5.0，然后相除得0.2；接着用（第3个字符-0.2）*第4个字符*16.0，得到结果。

4、继续向下分析，发现程序最终是将刚得到的结果与384.0比较，并将结果存入ax，并根据ax的值判断是否进行跳转



5、因此我们只要保证最后计算出的结果为384.0就可以了！很容易算出key=1555，运行验证！



6、因此注册机为：

```
# -*- coding:utf-8 -*-
while(1):
    str = raw_input("")
    #print type(str)
    if len(str) == 4:
        result = (int(str[2],10)-0.2)*int(str[3],10)*16.0
        if result == 384.0:
            print "Registration successful!"
        else:
            print "error!"
    else:
        print"error!"
```

```
1234
error!
1555
Registration successful!
```