看雪Q1流浪者 简单 wp

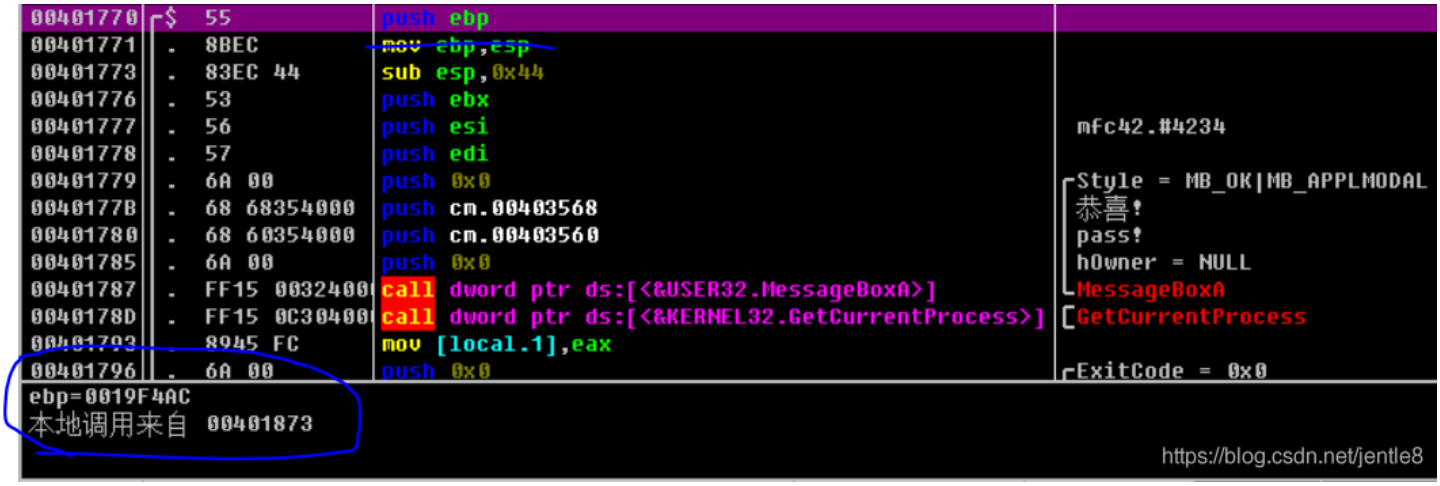
原创

菜鸟m号 于 2019-11-20 00:26:17 发布 132 收藏

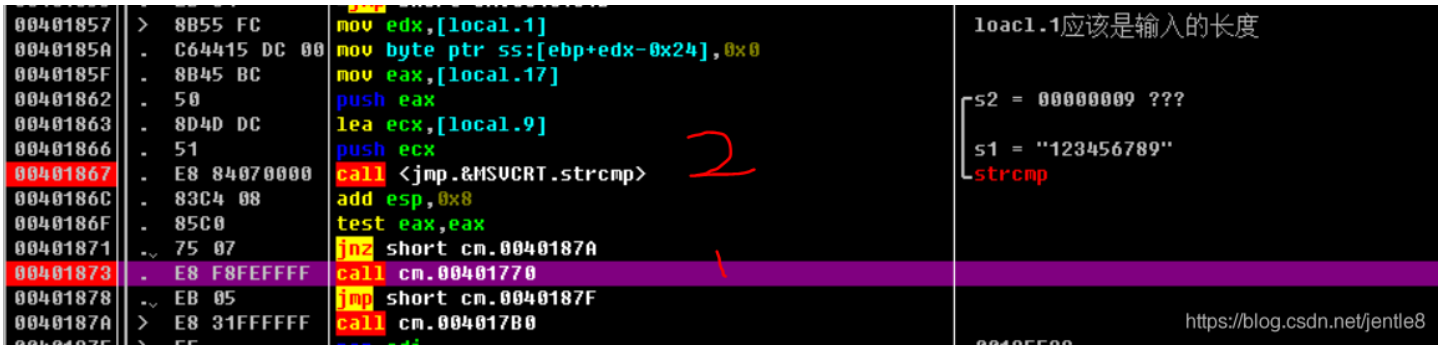
分类专栏： 逆向 文章标签： CTF 逆向

本文链接：https://blog.csdn.net/jentle8/article/details/103154045

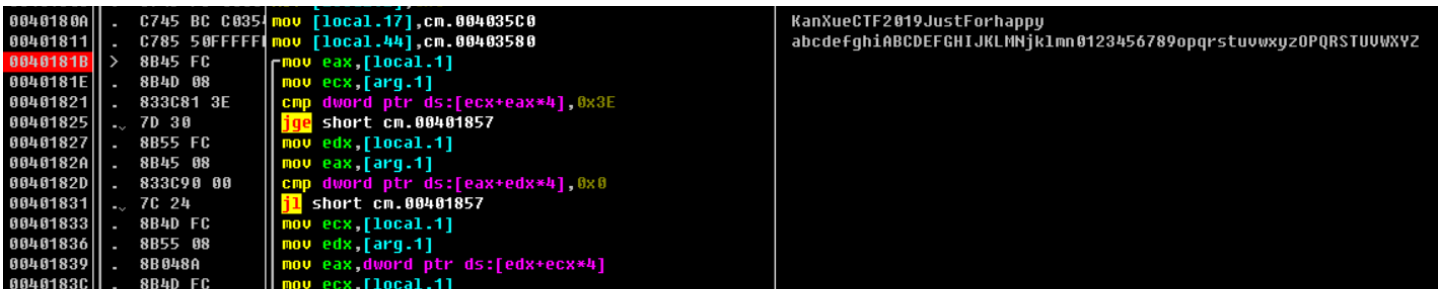
资源见上传文件，这里很多人使用ida进行静态分析，但是这样太依赖那个F5键了，我会用od进行一步步反调试得到keyGen.



先根据关键字符串得到主要跳转（我是这个办法），然后可以看到附近时一个简单的跳转语句：



只是定位到跳转还不行，往上稍微翻一下，就可以看到一个按照一个序列取出相对应ascii的操作，代码如下：



```
0040183F  .  8B95 50FFFFFF  mov edx,[local.44]
00401845  .  8A0402         mov al,byte ptr ds:[edx+eax]
00401848  .  88440D DC      mov byte ptr ss:[ebp+ecx-0x24],al
0040184C  .  8B4D FC        mov ecx,[local.1]
0040184F  .  83C1 01        add ecx,0x1
00401852  .  894D FC        mov [local.1],ecx
00401855  .^ EB C4          jmp short cm.0040181B
```


我一开始在这停留了比较久的时间，是因为我看到栈控件已经有输入的字符串，以为之前的是某一个函数得到用户输入的字符串就完事了。后来调试的时候不对，单纯的依据输入的字符串得到的下标值是取不到后面的大写字母和数字的 。然后根据栈回溯的方法，得到输入的处理函数。

```
00401908  >  8B55 F8        mov edx,[local.2]
0040190B  .  0355 F4        add edx,[local.3]
0040190E  .  0FBE02         movsx eax,byte ptr ds:[edx]
00401911  .  85C0           test eax,eax
00401913  .v 0F84 A6000000  je cm.004019BF
00401919  .  8B4D F8        mov ecx,[local.2]
0040191C  .  034D F4        add ecx,[local.3]
0040191F  .  0FBE11         movsx edx,byte ptr ds:[ecx]
00401922  .  83FA 39        cmp edx,0x39
00401925  .v 7F 23          jg short cm.0040194A
00401927  .  8B45 F8        mov eax,[local.2]
0040192A  .  0345 F4        add eax,[local.3]
0040192D  .  0FBE08         movsx ecx,byte ptr ds:[eax]
00401930  .  83F9 30        cmp ecx,0x30
00401933  .v 7C 15          jl short cm.0040194A
00401935  .  8B55 F8        mov edx,[local.2]
00401938  .  0355 F4        add edx,[local.3]
0040193B  .  0FBE02         movsx eax,byte ptr ds:[edx]
0040193E  .  83E8 30        sub eax,0x30
00401941  .  8B4D F4        mov ecx,[local.3]
00401944  .  89448D 8C      mov dword ptr ss:[ebp+ecx*4-0x74],eax
00401948  .v EB 67          jmp short cm.004019B1
0040194A  >  8B55 F8        mov edx,[local.2]
0040194D  .  0355 F4        add edx,[local.3]
00401950  .  0FBE02         movsx eax,byte ptr ds:[edx]
00401953  .  83F8 7A        cmp eax,0x7A
00401956  .  7F 23          jg short cm.0040197B
```


这个过程比较简单，就是如果是数字就减去0x30，是大写字母就0x1D，是小写字母就减去57
根据索引得到下表，和字符串进行比较。
keyTab[]='abcdefghiABCDEFGHIJKLMNjklmn0123456789opqrstuvwxyzOPQRSTUVWXYZ'
key[index]="KanXueCTF2019JustForhappy"

keyGen如下（太晚了这是别的大佬写的）：

```
string strs = "abcdefghiABCDEFGHIJKLMNjklmn0123456789opqrstuvwxyzOPQRSTUVWXYZ";
char Kanxue[] = "KanXueCTF2019JustForhappy";
size_t snIndex = 0;
for (int i = 0; i < 25; ++i)
{
    // 获取字符在字符串中下标
    snIndex = strs.find(Kanxue[i]);

    // 通过随机匹配
    if (snIndex + 0x57 >= 'a' && snIndex + 0x57 <= 'z')
        printf("%c", snIndex + 0x57);

    if (snIndex + 0x30 >= '0' && snIndex + 0x30 <= '9')
        printf("%c", snIndex + 0x30);

    if (snIndex + 0x1D >= 'A' && snIndex + 0x1D <= 'Z')
        printf("%c", snIndex + 0x1D);
}
```

```
C:\Users\Administrator\source\repos\ConsoleApplication3\D
j0rXI4bTeustBiIGHeCF70DDM
请按任意键继续. . .
```