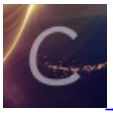
【reversing.kr逆向之旅】Music Player的writeup

原创

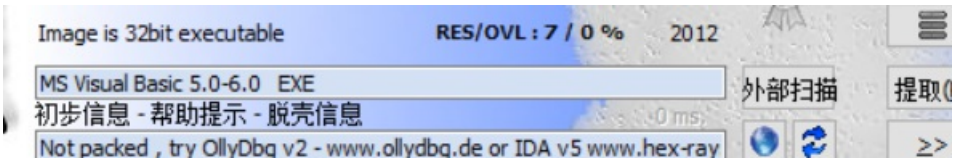
iqiqiya 于 2018-11-01 16:48:30 发布 400 收藏
分类专栏： 我的逆向之路 ------reversing.kr 我的CTF之路 文章标签： 【reversing.kr逆向之旅】Music Player reversing.kr Music Player的wri Music Player的writeup


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


------reversing.kr
11 篇文章 0 订阅
订阅专栏

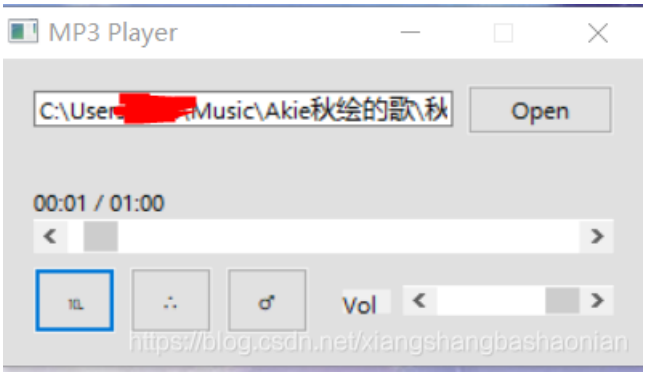

我的CTF之路
92 篇文章 5 订阅
订阅专栏

VB写的程序 且没有加壳

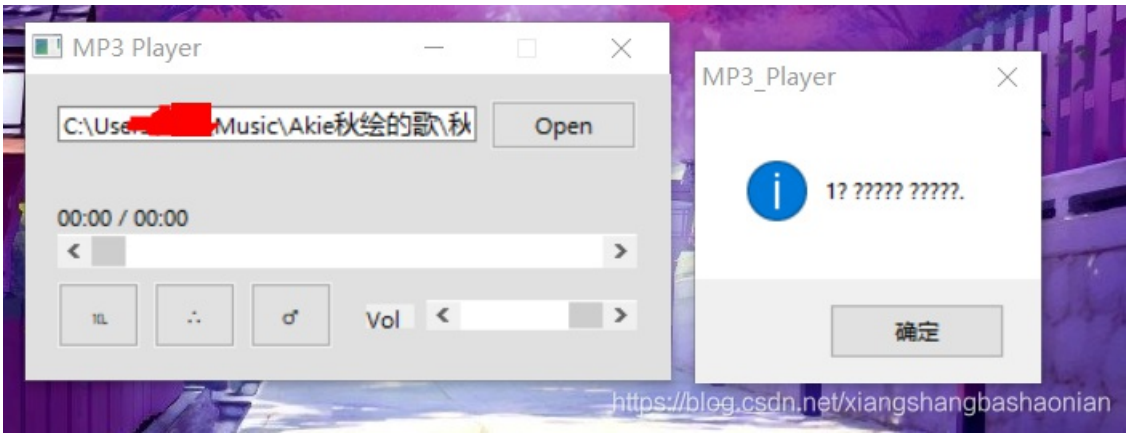


运行看看 还真是一个音乐播放器 但是只能播放一分钟

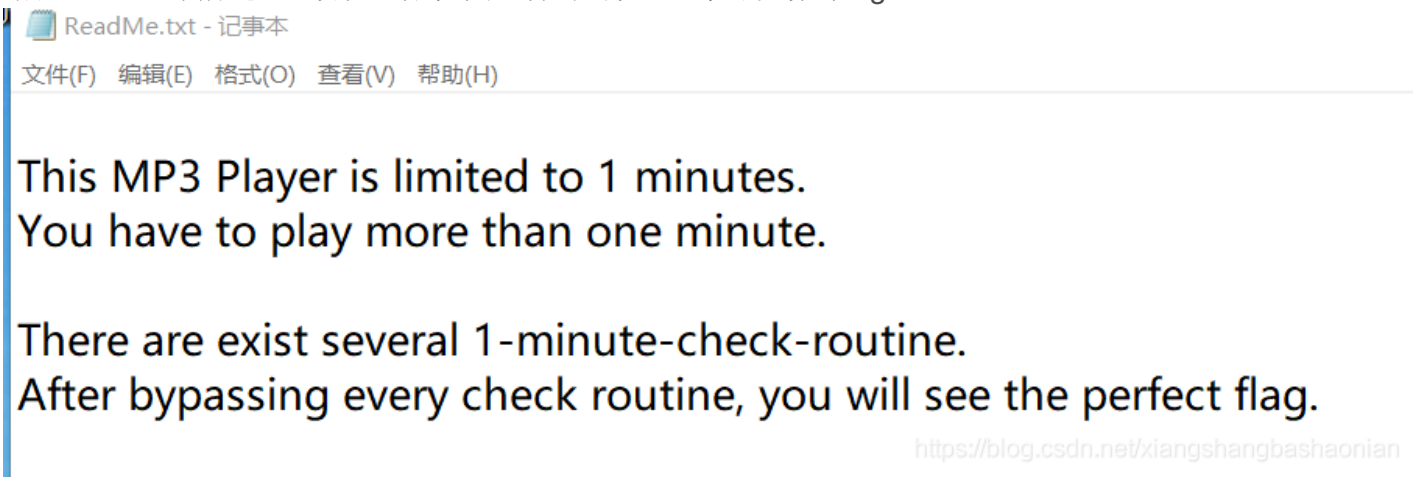
下面三个按钮据我分析 分别就是播放，暂停，重新开始播放



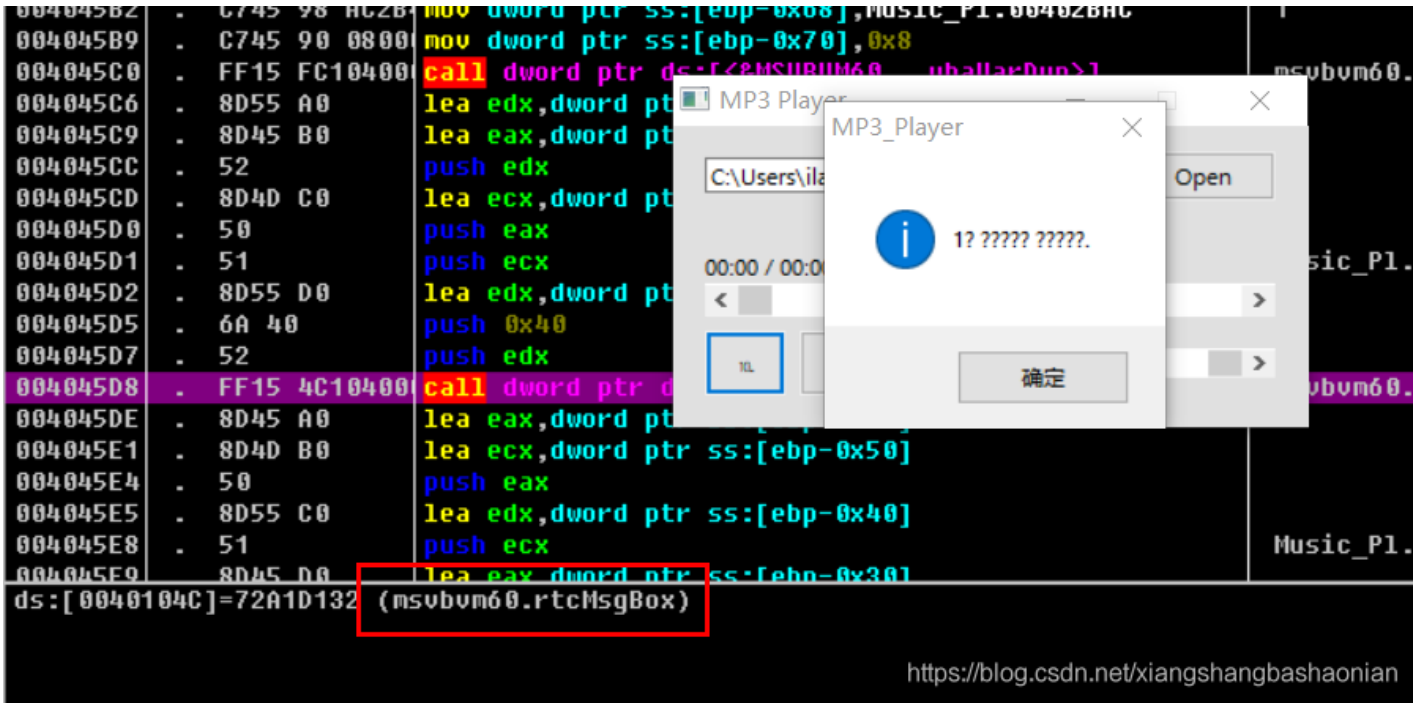
当滑动到1分钟时就会停止 并弹窗1？ ?????



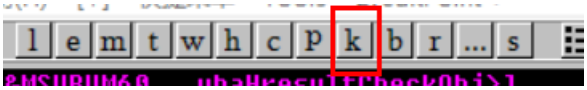
结合ReadMe中所述　必须跳过若干个在1分钟的检查　才可以看到flag



OD载入分析　F9运行　播放到1分钟时弹窗　这时候可以看到程序调用了rtcMsgBox



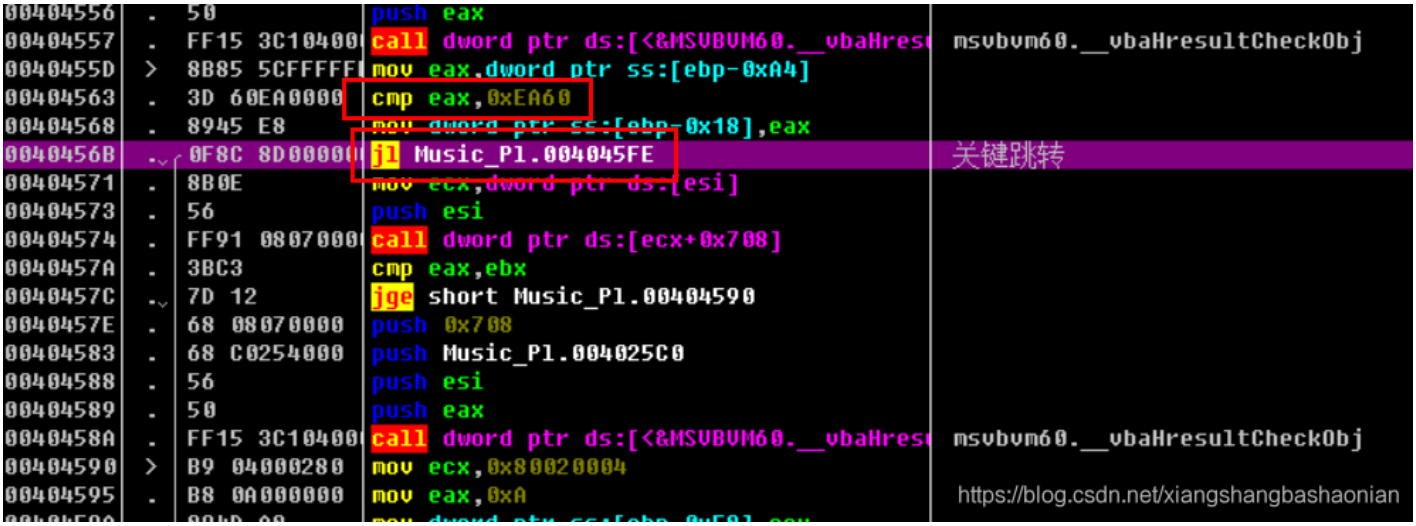
这时候点击k查看调用堆栈情况　可以看到有调用rtcMsgBox这个API



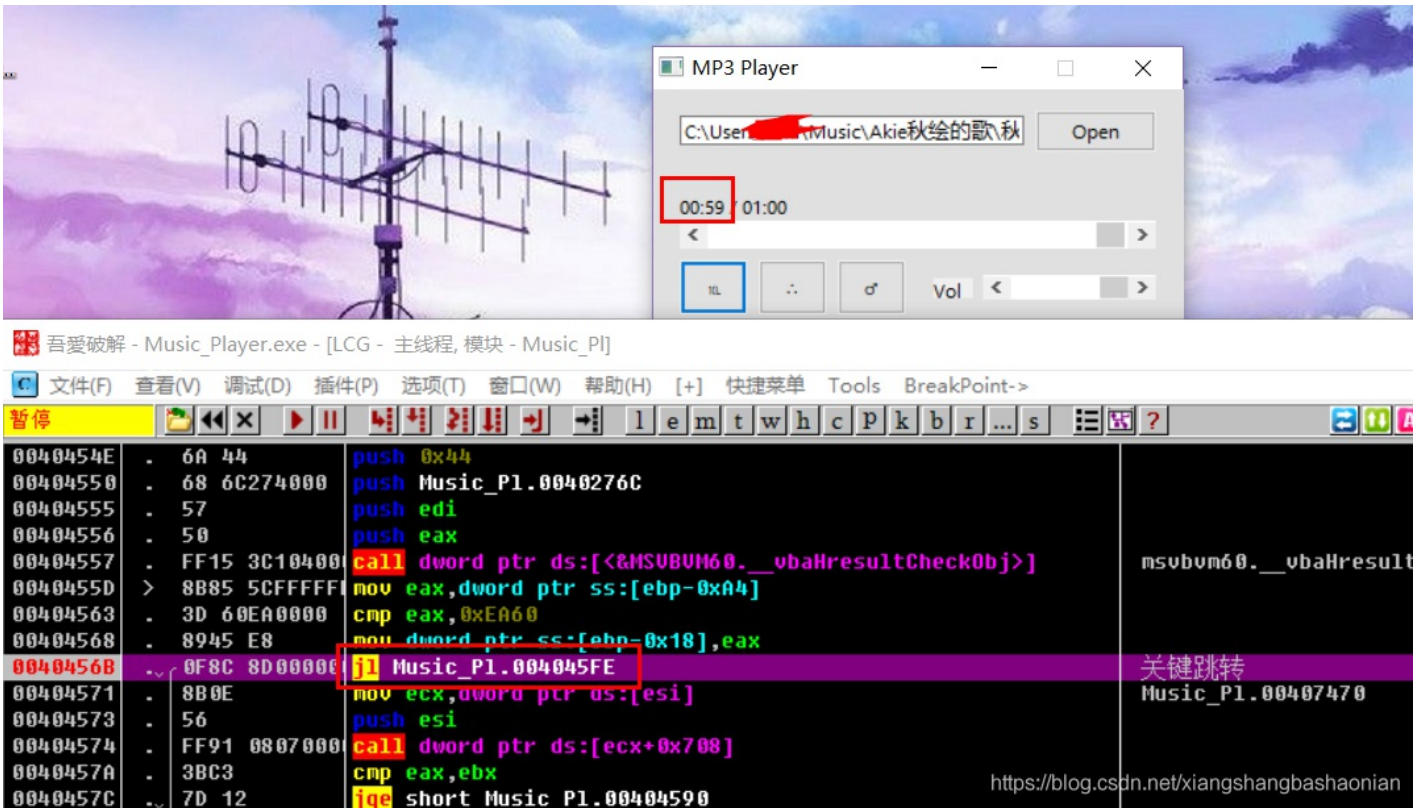
接着右键这一行 查看调用

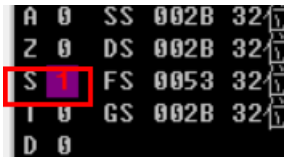
向上翻 可以很明显发现cmp

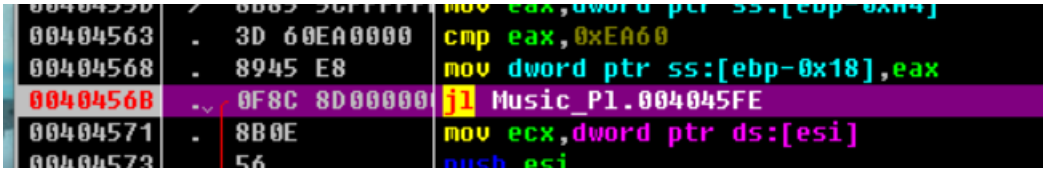
0xEA60 就是60000毫秒 正好就是1分钟 而且这个跳转正好跳过.rtcMsgBox 猜测这个就是关键跳



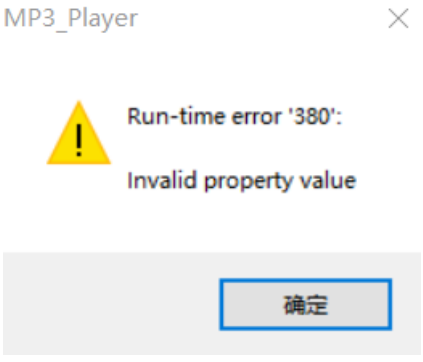
这里的话修改下s标志位 使跳转成立







接着发现还是会报错



也是醉了

猜测下面还有校验判断的地方　重新来一次　这次修改过s标志位后　单步向下　看看到底是何方神圣。。

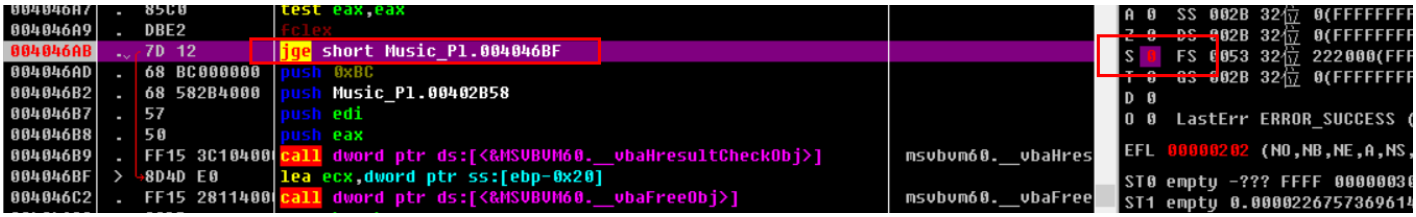
然后很明显可以看到当经过这个call后　就会弹窗报错

还可以看到上边有一个jge跳转　　这时候我们可以把它改为jmp　或者再次修改s标志位

```
004046B9   .  FF15 3C104000 call dword ptr ds:[<&MSVBVM60.__vbaHresultCheckObj>]        ;  msvbvm60.__vbaHr
```

```
0040467C  .  50            push eax
0040467D  .  8D45 E0       lea eax,dword ptr ss:[ebp-0x20]
00404680  .  50            push eax
00404681  .  FF15 4810400( call dword ptr ds:[<&MSVBVM60.__vbaObjSet>]      msvbvm60.__vbaObjSet
00404687  .  8BF8          mov edi,eax
00404689  .  8BCB          mov ecx,ebx
0040468B  .  8B17          mov edx,dword ptr ds:[edi]
0040468D  .  8995 40FFFFFF mov dword ptr ss:[ebp-0xC0],edx
00404693  .  FF15 8410400( call dword ptr ds:[<&MSVBVM60.__vbaI2I4>]       msvbvm60.__vbaI2I4
00404699  .  8B8D 40FFFFFF mov ecx,dword ptr ss:[ebp-0xC0]
0040469F  .  50            push eax
004046A0  .  57            push edi
004046A1  .  FF91 BC00000( call dword ptr ds:[ecx+0xBC]
004046A7  .  85C0          test eax,eax
004046A9  .  DBE2          fclex
004046AB  .  7D 12         jge short Music_P1.004046BF
004046AD  .  68 BC000000   push 0xBC
004046B2  .  68 582B4000   push Music_P1.00402B58
004046B7  .  57            push edi
004046B8  .  50            push eax
004046B9  .  FF15 3C1040(  call dword ptr ds:[<&MSVBVM60.__vbaHresultCheckObj>]  msvbvm60.__vbaHresultCheckObj
004046BF  >  8D4D E0       lea ecx,dword ptr ss:[ebp-0x20]
004046C2  .  FF15 2811400( call dword ptr ds:[<&MSVBVM60.__vbaFreeObj>]    msvbvm60.__vbaFreeObj
004046C8  .  33DB          xor ebx,ebx
004046CA  >  8B46 34       mov eax,dword ptr ds:[esi+0x34]
004046CD  .  8D7E 34       lea edi,dword ptr ds:[esi+0x34]
跳转未实现
004046BF=Music_P1.004046BF
                                                  https://blog.csdn.net/xiangshangbashaonian
```

我还是选择修改s标志位(ps:建议直接改成jmp吧)

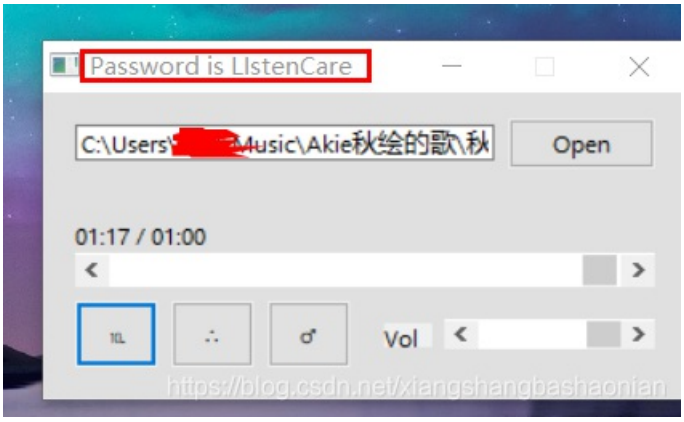


标题就是flag

LIstenCare

我把两处都改成jmp并且保存了一份 哈哈

终于可以安静的听秋绘女神唱歌啦



总结：VB程序中，rtcMsgBox 用于弹出一个消息框,类似于WINDOWS API中的MessageBoxA/MessageBoxExA函数