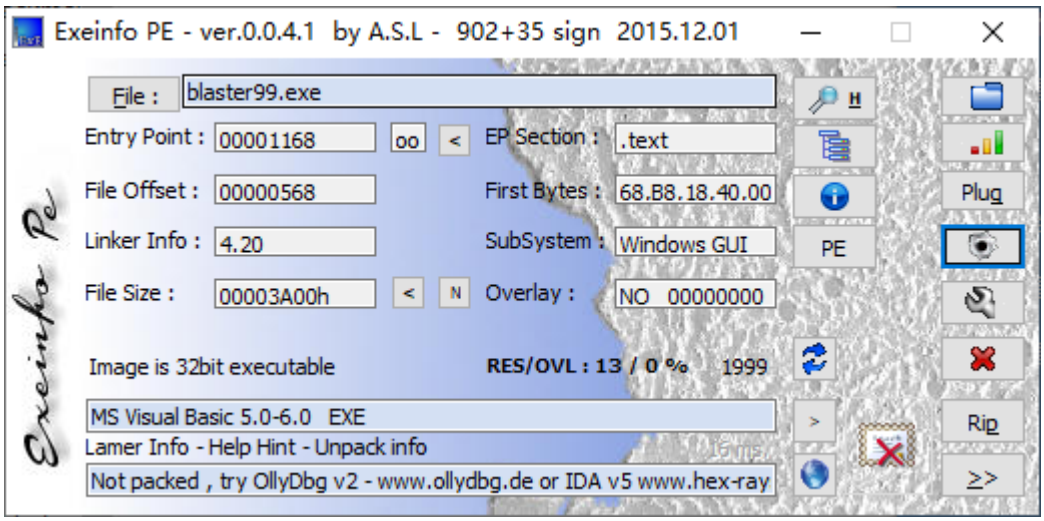
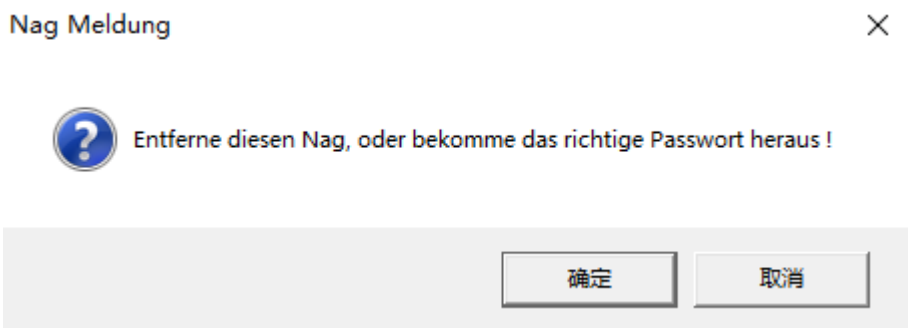
查壳



首先来查一下壳，又是个VB的程序，最近几个Crackme都是VB的，逆的我都想吐了，这个Crackme有两个任务，一个是去Neg，一个是找序列号，两个都比较简单

去Neg



首先要把这个弹框给去掉，直接搜索字符串，找到相应的位置，当然，也可以在rtcMsgBox函数下断点

```
00402C76  .  8975 AC      mov dword ptr ss:[ebp-0x54],esi
00402C79  .  8975 9C      mov dword ptr ss:[ebp-0x64],esi
00402C7C  .  8975 8C      mov dword ptr ss:[ebp-0x74],esi
00402C7F  .  89B5 5CFFFFFF mov dword ptr ss:[ebp-0xA4],esi
00402C85  .  C745 84 F01E4 mov dword ptr ss:[ebp-0x7C],blaster9.004  Entferne diesen Nag, oder bekomme das richtige Passw
00402C8C  .  899D 7CFFFFFF mov dword ptr ss:[ebp-0x84],ebx
00402C92  .  E8 95E4FFFF  call <jmp.&MSVBVM50.__vbaVarCopy>
00402C97  .  6A 03        push 0x3
00402C99  .  8D95 7CFFFFFF lea edx,dword ptr ss:[ebp-0x84]
00402C9F  .  5F           pop edi                          0019FABC
00402CA0  .  8D4D DC      lea ecx,dword ptr ss:[ebp-0x24]
00402CA3  .  C745 84 2100( mov dword ptr ss:[ebp-0x7C],0x21
00402CAA  .  89BD 7CFFFFFF mov dword ptr ss:[ebp-0x84],edi
00402CB0  .  E8 71E4FFFF  call <jmp.&MSVBVM50.__vbaVarMove>
00402CB5  .  8D95 7CFFFFFF lea edx,dword ptr ss:[ebp-0x84]
00402CBB  .  8D4D CC      lea ecx,dword ptr ss:[ebp-0x34]
```

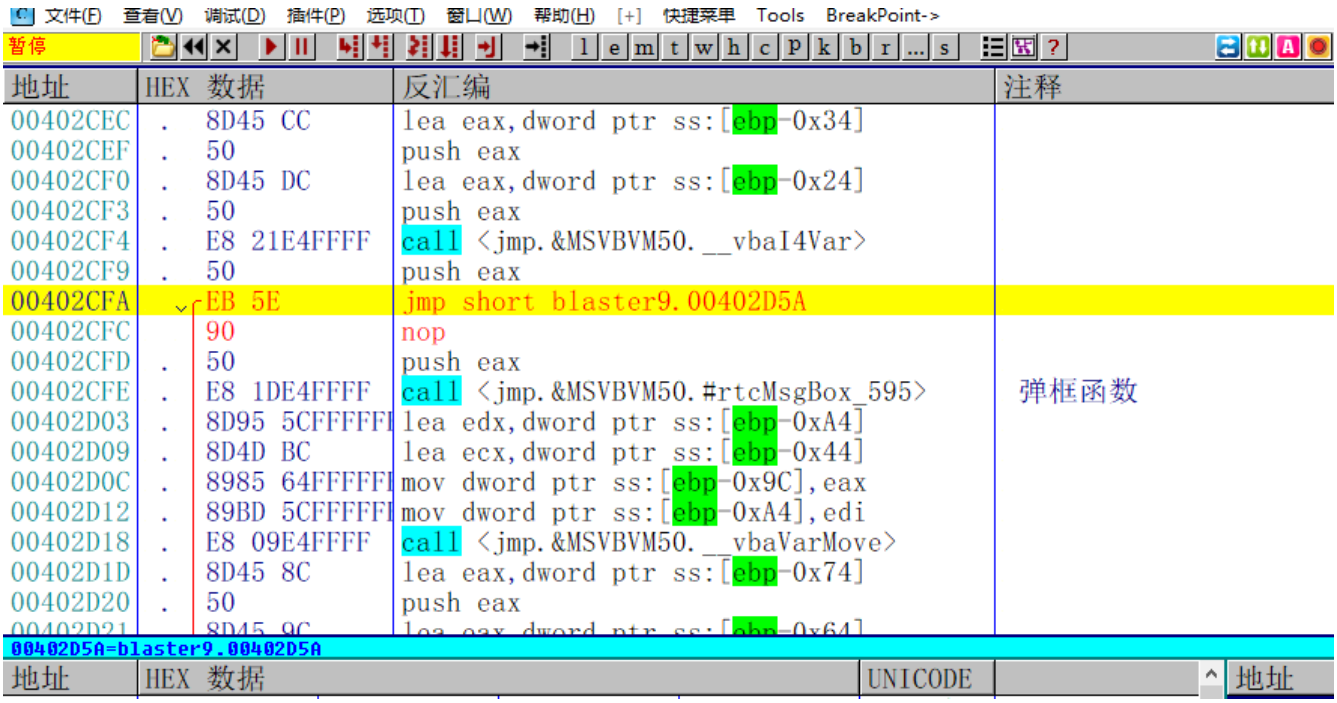
找到字符串位置之后往下拉，就能看到这个弹框的函数

地址	HEX 数据	反汇编	注释
00402CF0	. 8D45 DC	lea eax,dword ptr ss:[ebp-0x24]	
00402CF3	. 50	push eax	
00402CF4	. E8 21E4FFFF	call <jmp.&MSVBVM50.__vbaI4Var>	
00402CF9	. 50	push eax	
00402CFA	8D45 AC	lea eax,dword ptr ss:[ebp-0x54]	
00402CFD	. 50	push eax	
00402CFE	. E8 1DE4FFFF	call <jmp.&MSVBVM50.#rtcMsgBox_595>	弹框函数
00402D03	. 8D95 5CFFFFFF	lea edx,dword ptr ss:[ebp-0xA4]	
00402D09	. 8D4D BC	lea ecx,dword ptr ss:[ebp-0x44]	
00402D0C	. 8985 64FFFFFF	mov dword ptr ss:[ebp-0x9C],eax	
00402D12	. 89BD 5CFFFFFF	mov dword ptr ss:[ebp-0xA4],edi	
00402D18	. E8 09E4FFFF	call <jmp.&MSVBVM50.__vbaVarMove>	
00402D1D	. 8D45 8C	lea eax,dword ptr ss:[ebp-0x74]	

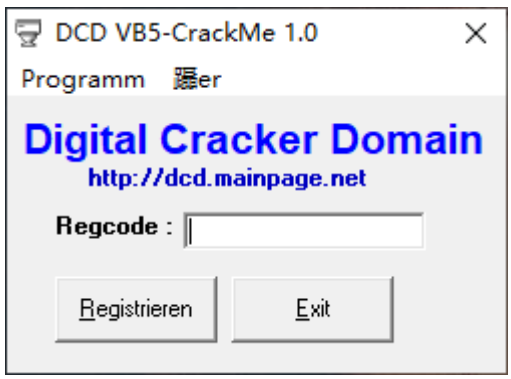
然后会判断返回值，点击确定则继续走程序流程，否则退出程序

```
00402D32  .  C745 84 0100( mov dword ptr ss:[ebp-0x7C],0x1
00402D39  .  C785 7CFFFFFF mov dword ptr ss:[ebp-0x84],0x8003
00402D43  .  50           push eax                         var18 = FFFFFFFF
00402D44  .  8D85 7CFFFFFF lea eax,dword ptr ss:[ebp-0x84]
00402D4A  .  50           push eax                         var28 = FFFFFFFF
00402D4B  .  E8 BEE3FFFF  call <jmp.&MSVBVM50.__vbaVarTstEq>  __vbaVarTstEq
00402D50  .  66:85C0      test ax,ax                       判断是确定还是取消
00402D53  .v 75 05        jnz short blaster9.00402D5A
00402D55  .  E8 AEE3FFFF  call <jmp.&MSVBVM50.__vbaEnd>    取消则退出程序
00402D5A  >  8975 FC      mov dword ptr ss:[ebp-0x4],esi
00402D5D  .  68 982D4000  push blaster9.00402D98
00402D62  .v EB 13        jmp short blaster9.00402D77
00402D64  .  8D45 8C      lea eax,dword ptr ss:[ebp-0x74]
00402D67  .  50           push eax
```

那么去掉这个Neg就很简单了 在弹框之前直接让程序跳到0x402D5A这个位置，修改后如下



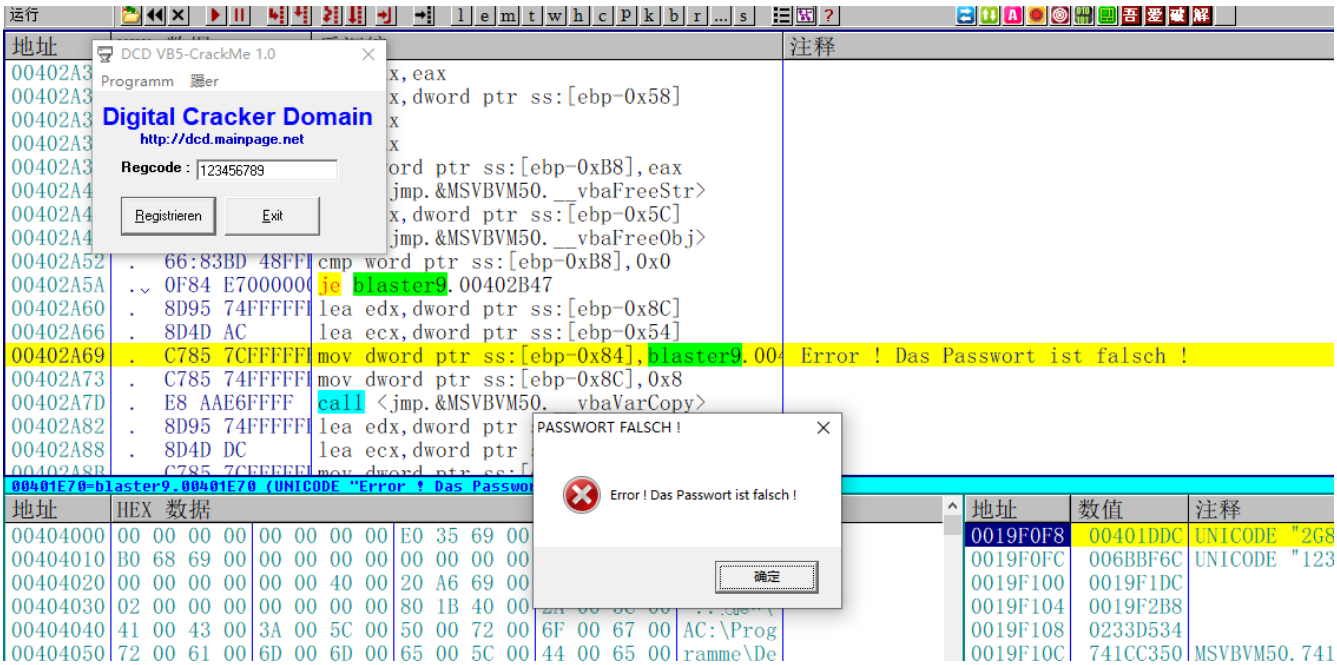
修改完成之后保存文件



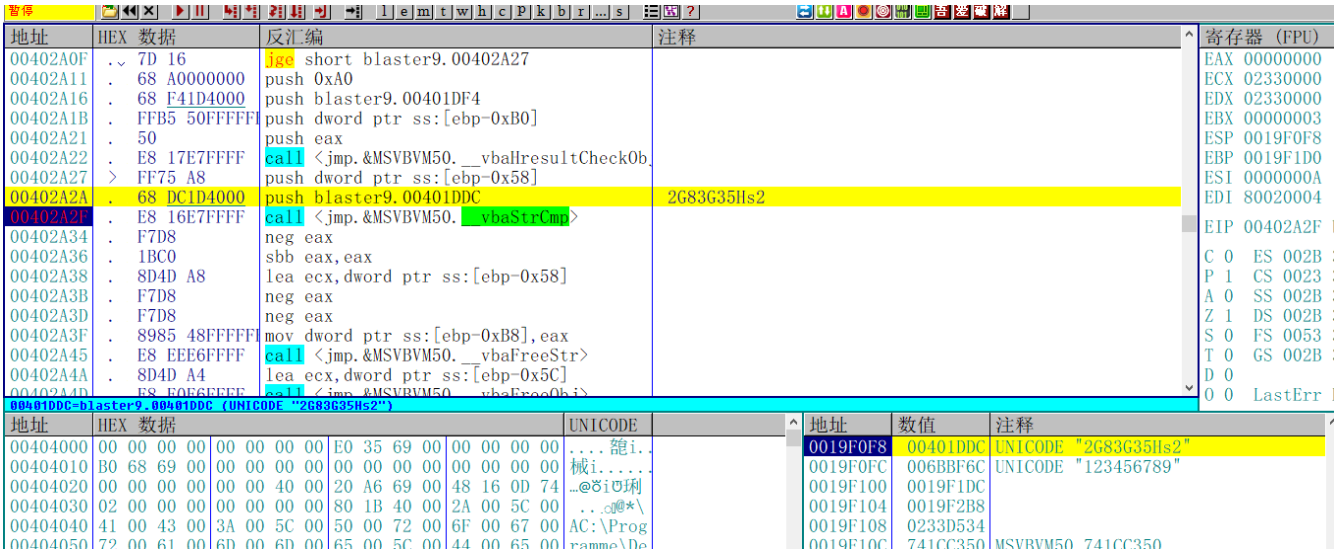
弹框完美去除

破解序列号

接下来还是从字符串入手追踪序列号



往上拉，发现一个vbaStrCmp函数，将输入的序列号和一个字符串比较，那么这个应该就是正确的序列号了



校验结果

输入**2G83G35Hs2**，提示成功，破解完成

需要相关文件的可以到我的Github下载：https://github.com/TonyChen56/160-Crackme