《漏洞利用及渗透测试基础》实验报告

姓名：孙蕗 学号：2112060 班级：信安1班

**实验名称：**

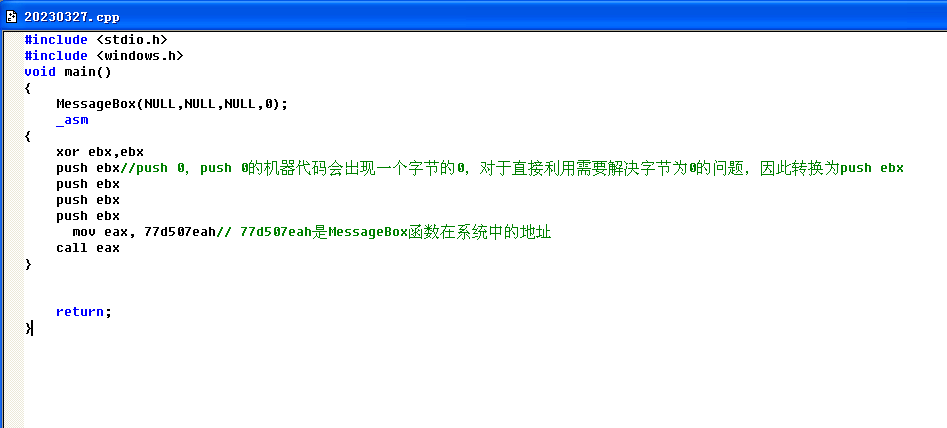
shellcode编写及编码

**实验要求：**

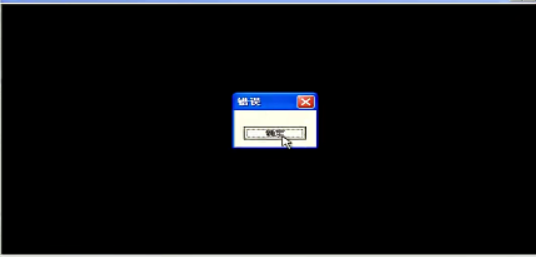
复现第五章实验三，并将产生的编码后的shellcode在示例5-4中进行验证，阐述shellcode编码的原理、shellcode提取的思想。

**实验过程：**

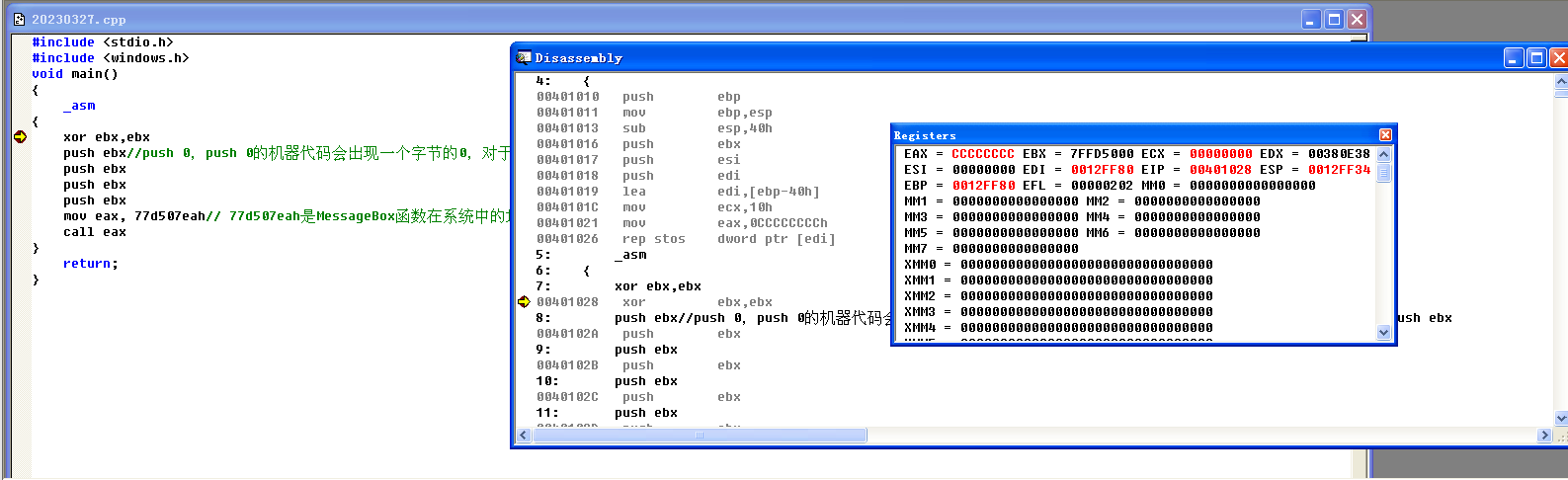
1. 编写代码



1. 运行为空

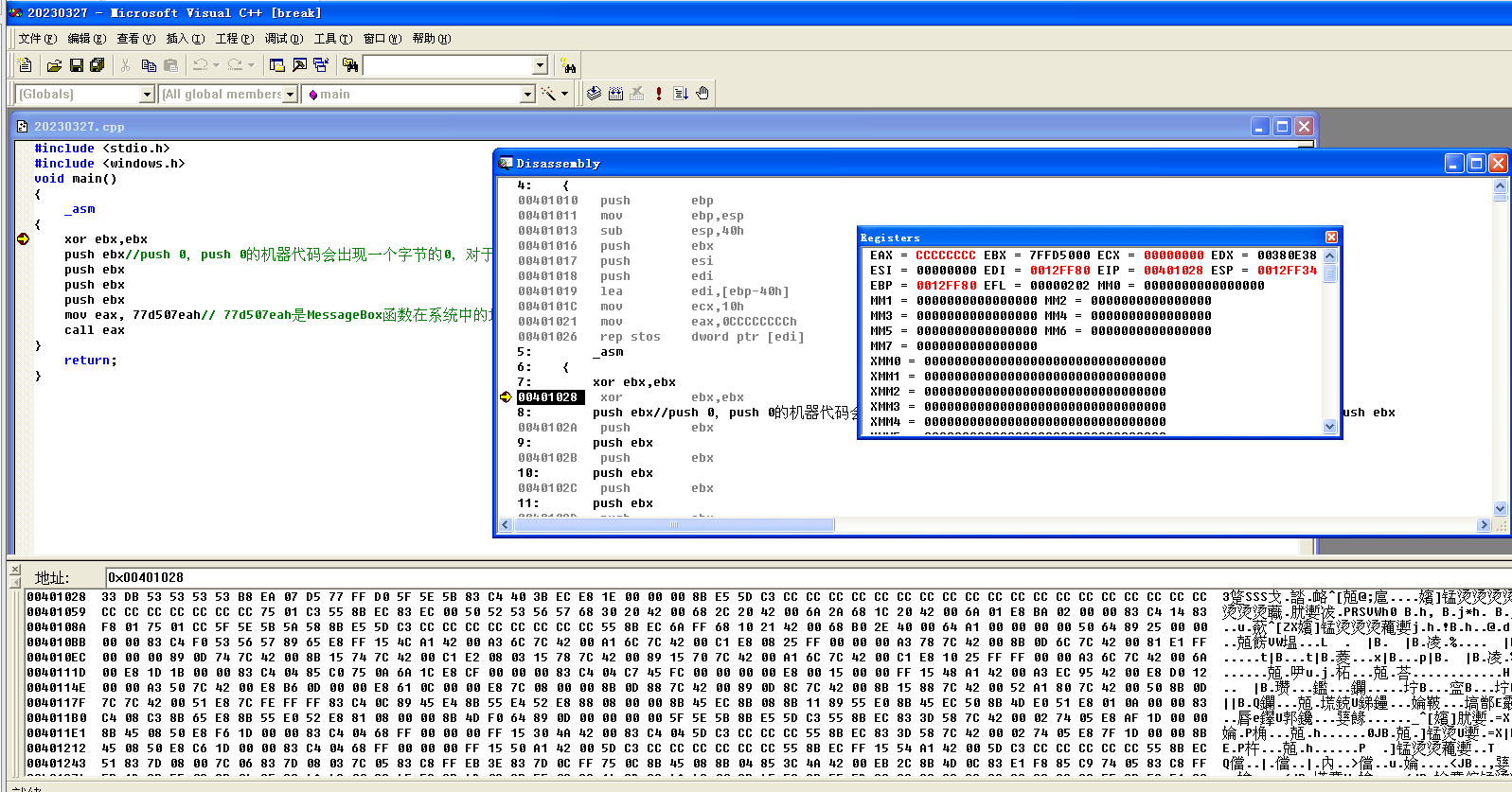


1. F9打断点，转到反汇编，F10调试

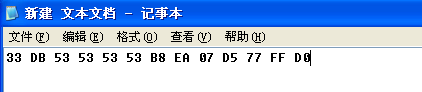


查看地址，从00401028开始，到00401035之前结束

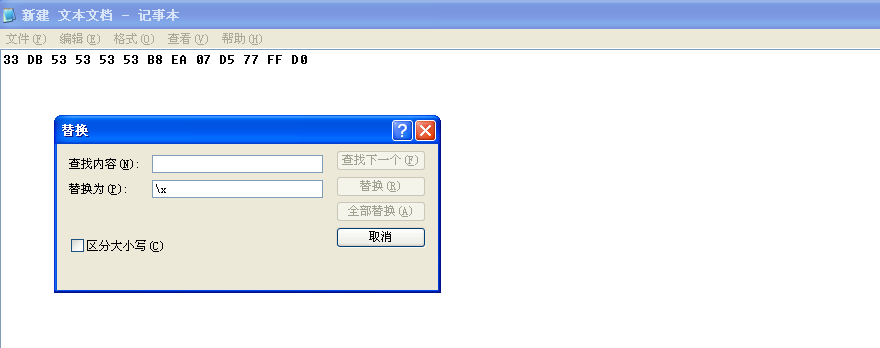
1. 地址是00401028，查看00401028



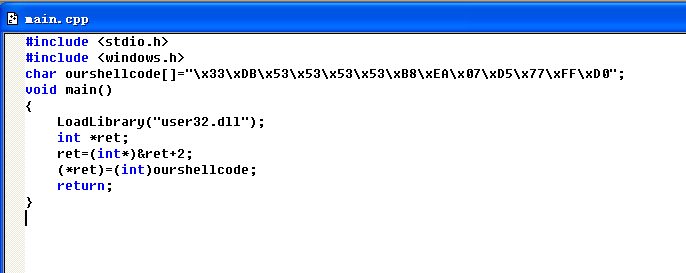
1. 00401028-00401034地址，复制机器码33 DB 53 53 53 53 B8 EA 07 D5 77 FF D0



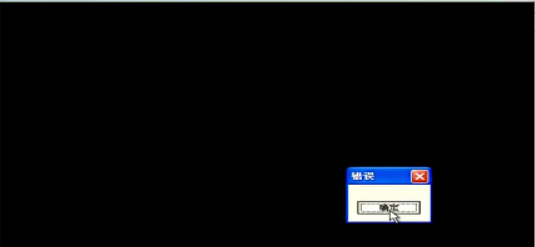
1. 处理机器码，编辑->替换，空格替换成/x

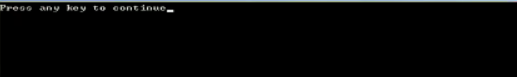


1. 机器码处理成16进制数



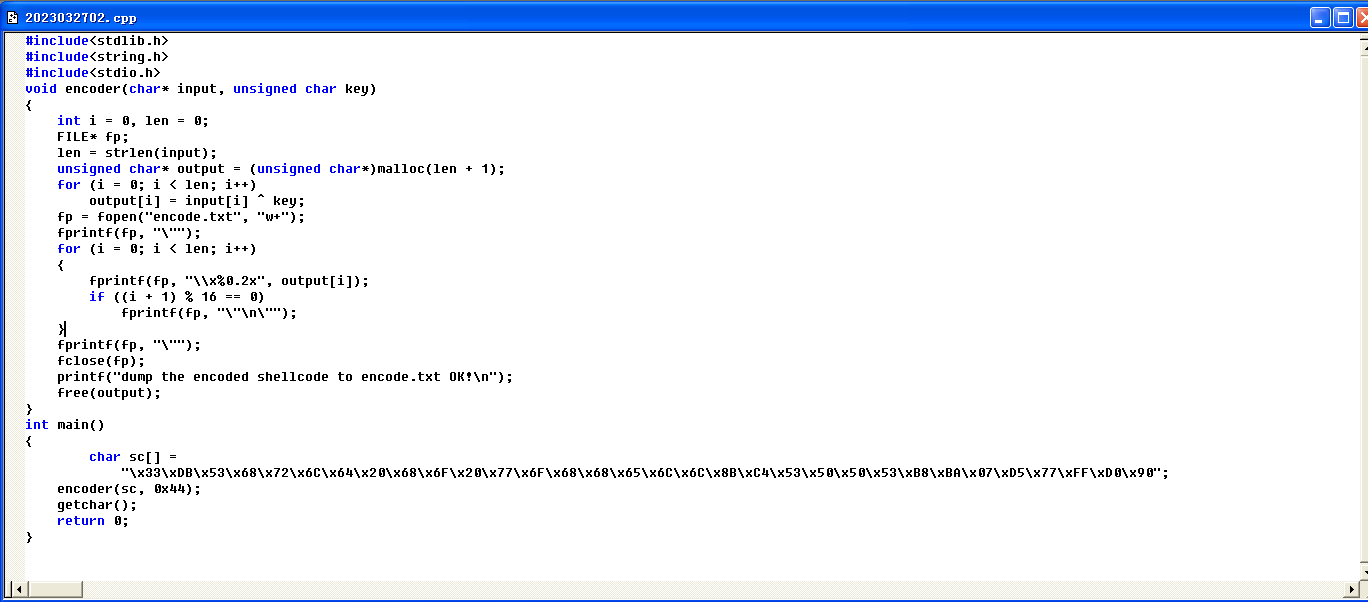
1. 验证





写的shellcode能够调用messagebox函数

1. 编码程序，将shellcode代码输入后，输出异或后的shellcode代码

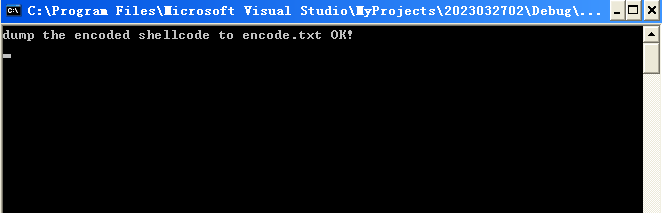


编码程序里有一个编码器，有一个主函数。

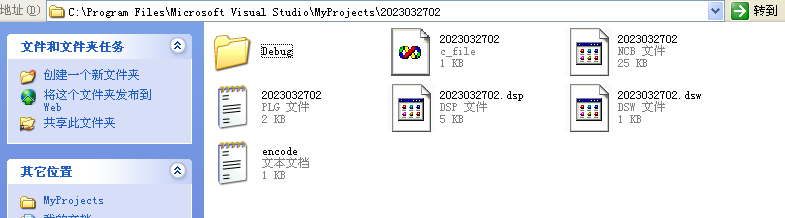
主函数里输入编码的对象，char sc[]="\x33\xDB\x53\x68\x72\x6C\x64\x20\x68\x6F\x20\x77\x6F\x68\x68\x65\x6C\x6C\x8B\xC4\x53\x50\x50\x53\xB8\xBA\x07\xD5\x77\xFF\xD0\x90";

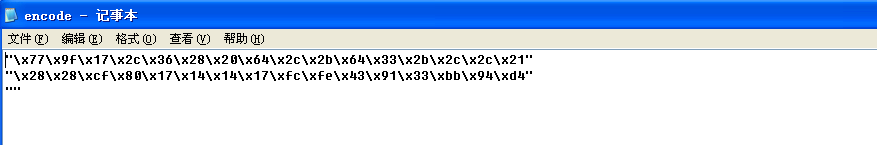
encoder函数完成编码，0x44作为秘钥。对输入的没一个字节进行异或，放到输出output[]里，输出写到一个文件里。

1. 执行



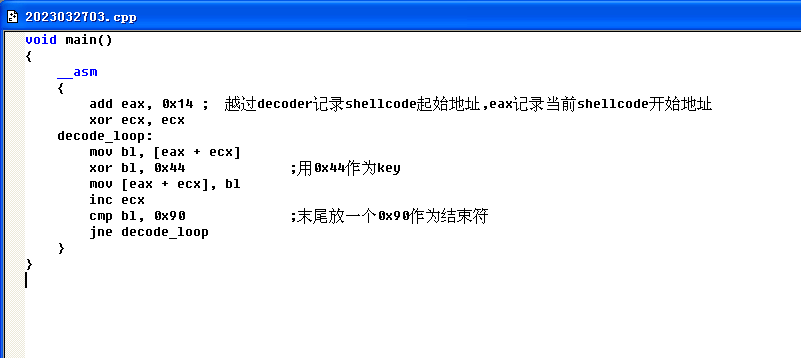
1. 打开文件夹，查看encode





encode.txt里是编码后的shellcode

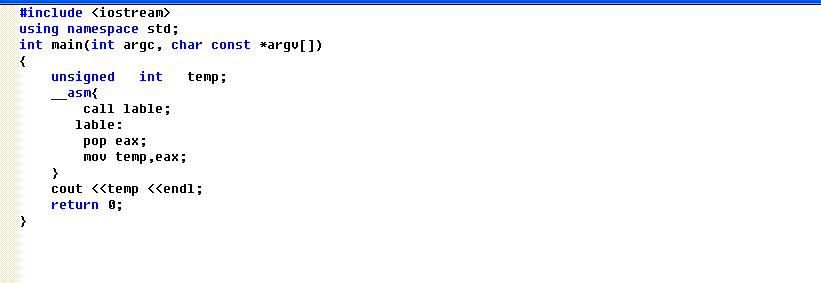
1. 写解码程序

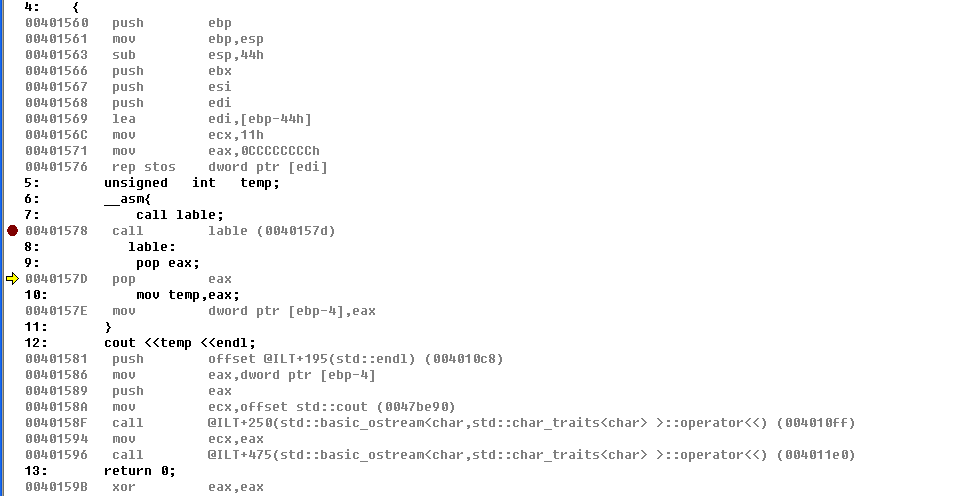


eax是当前这条指令的起始地址，这一段汇编指令总长0x14，eax执行后将指向这段指令后的下一段地址。xor ecx,ecx将ecx=0。decode\_loop前三行将解码字节取出，解码后再放回去。

inc ecx每一次解码后+1。cmp bl,0x90 末尾应该有一个0x90作为结束符。

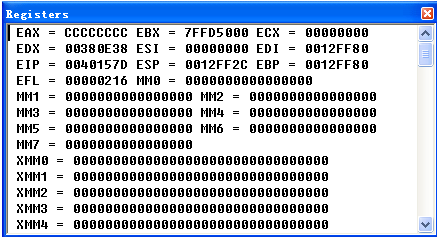
1. 为让eax记录shellcode当前的起始地址，获得代码当前指令地址，获取反汇编代码查看地址

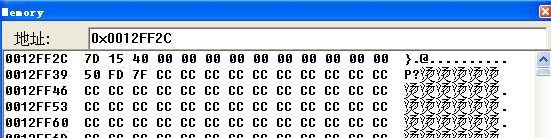




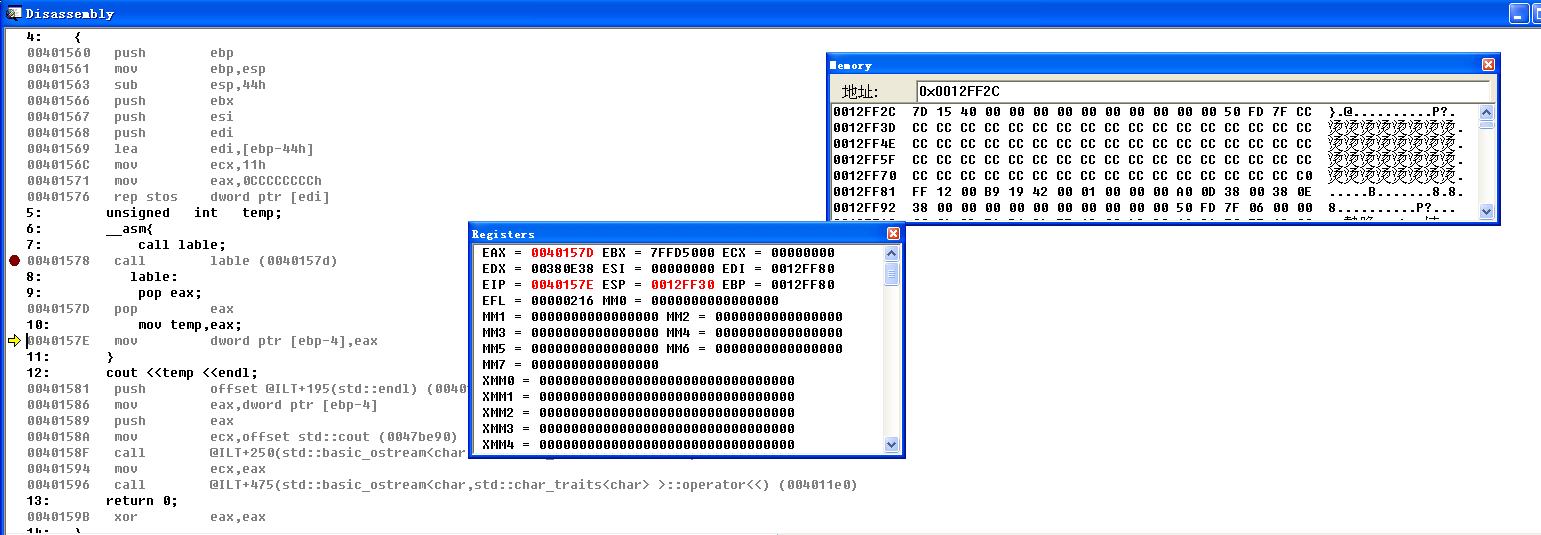
call指令将当前函数的下一条指令的地址作为返回值入栈，即0040157D。

此时esp=0012FF2C，eip=0040157D，已经入栈



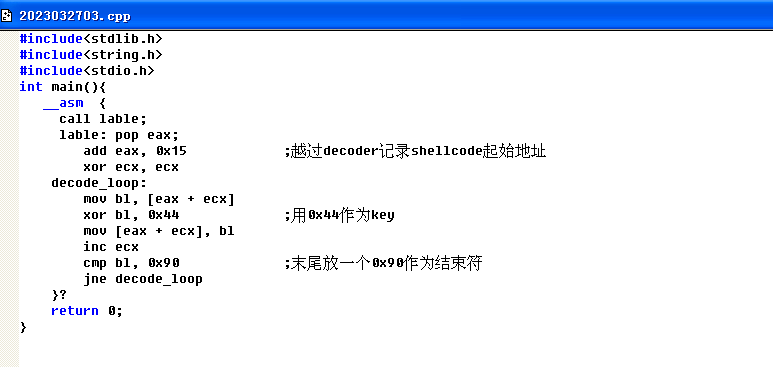


1. F10

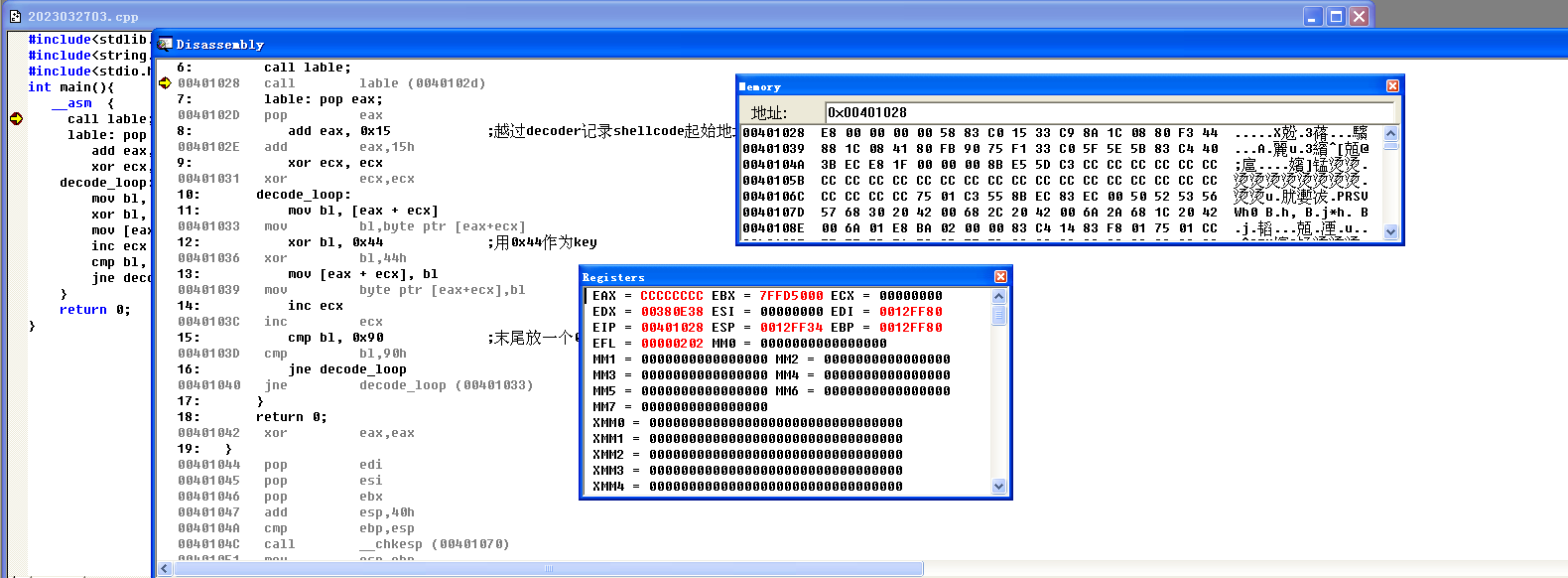


eax=0040157D。eax记录的是shellcode当前的起始地址

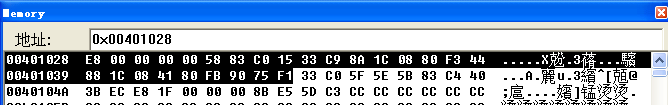
1. 合在一起



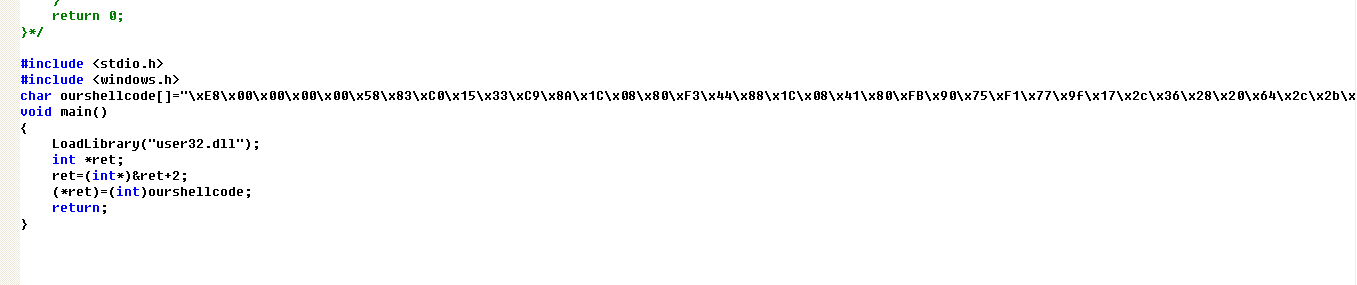
反汇编查看



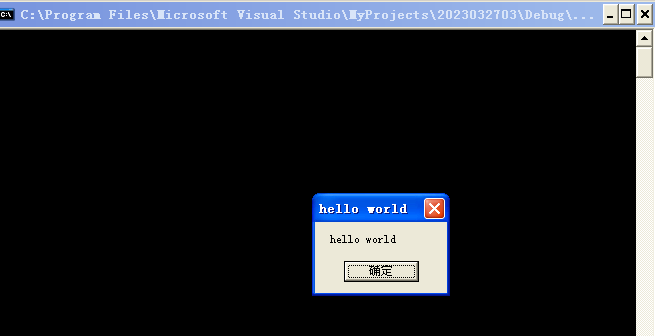
到00401041结束



1. 再加上encode.txt里编码后的shellcode，最后形成带解码程序的完整的shellcode



1. 进行验证



**心得体会：**

利用溢出覆盖返回地址，转去执行植入的恶意程序。Shellcode编码的原理是通过将目标机器的汇编代码转换成机器码，并将它们放入缓冲区中，以便能够被执行。Shellcode代码植入需要依次获取函数地址，编写函数调用的汇编代码，注入shellcode代码。

Shellcode代码编写需要对特定字符需要转码，函数API定位也很困难。Shellcode提取的思想是将写好的Shellcode程序转换成二进制代码，并将其注入到目标程序中进行攻击。具体而言，需要先将Shellcode程序编写成适合目标机器的代码，并使用工具将其转换成二进制代码。然后，在攻击时需要将这些二进制代码注入到目标程序中，使其被执行。

为编写shellcode代码，可依次用c语言书写要执行的Shellcode，换成对应的汇编代码，最后根据汇编代码，找到对应地址中的机器码。对于网页shellcode，可以采用base64编码；对二进制机器码，可采用自定义编码，如异或编码、计算编码、简单加解密等方法进行shellcode编码。