《shellcode编码解码》实验报告

姓名：汤清云 学号：2013536 班级： 1075

**实验名称：**

Shellcode编码解码实验。

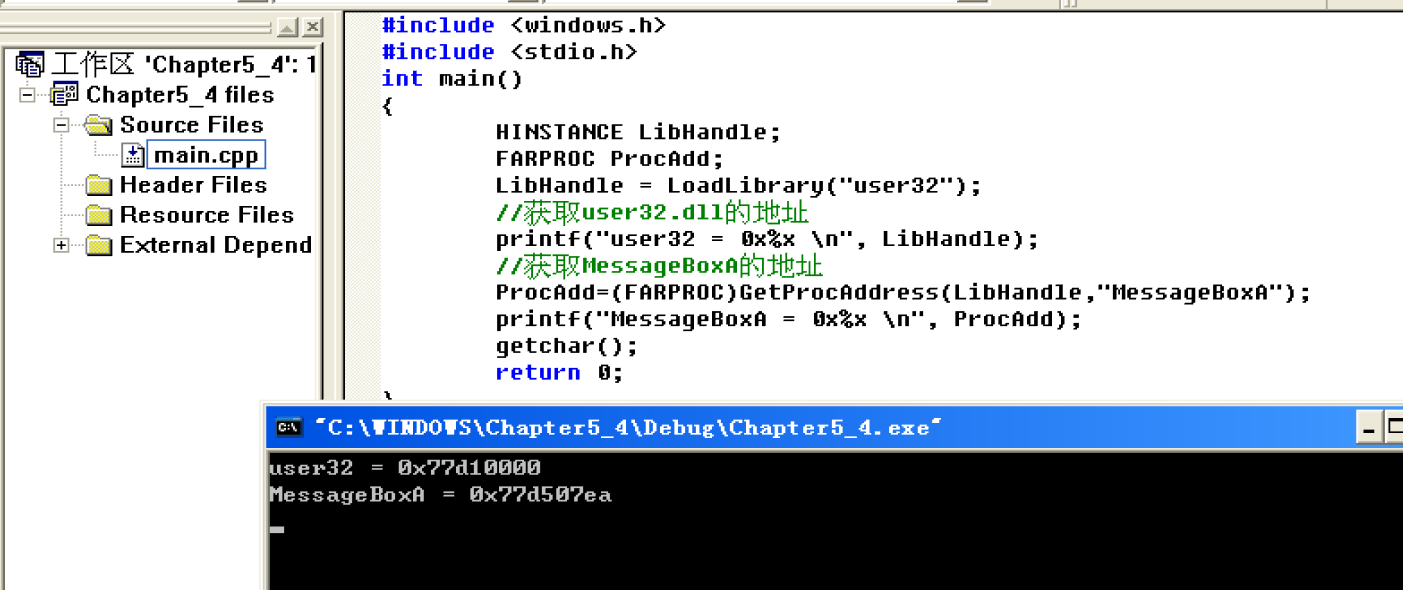
**实验要求：**

复现第五章实验三（就是能够利用异或解码程序实现弹出对话框的上课讲的内容），并将产生的编码后的shellcode在示例5-4（见上述代码）中进行验证，阐述shellcode编码的原理、shellcode提取的思想。

**实验过程：**

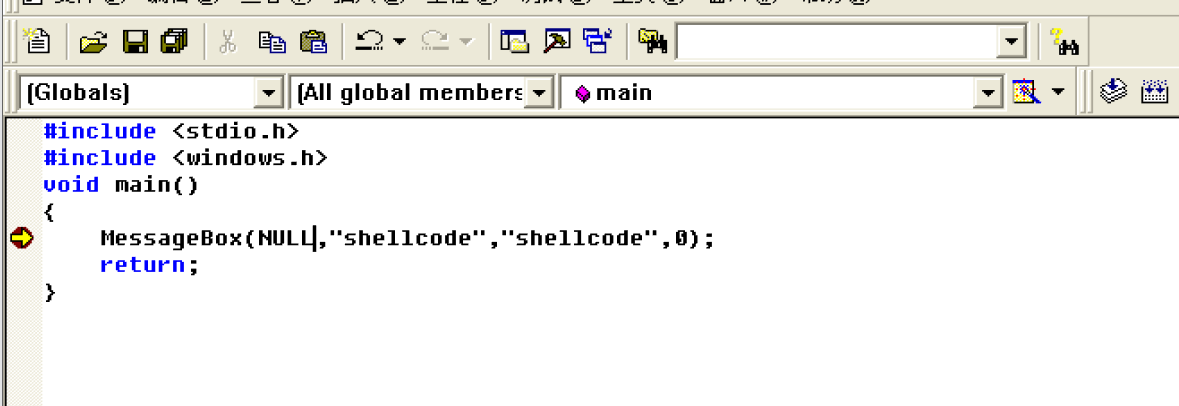
1. Shellcode编写方法

第一步：获取messagebox函数地址。

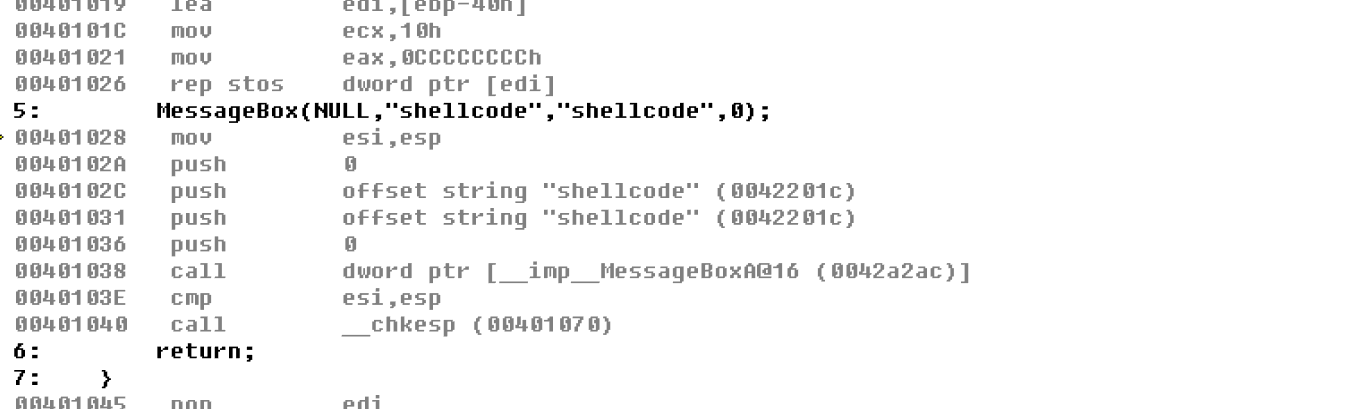


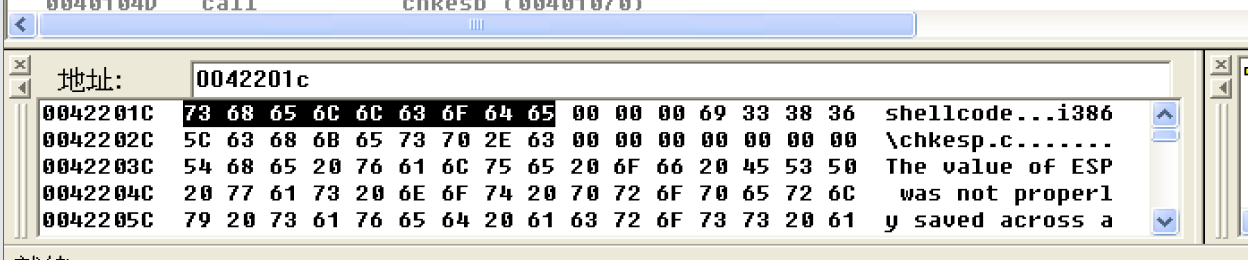
得到MessageBoxA函数在内存中的入口地址：0x77D507EA。

第二步：用c语言书写要执行的shellcode。



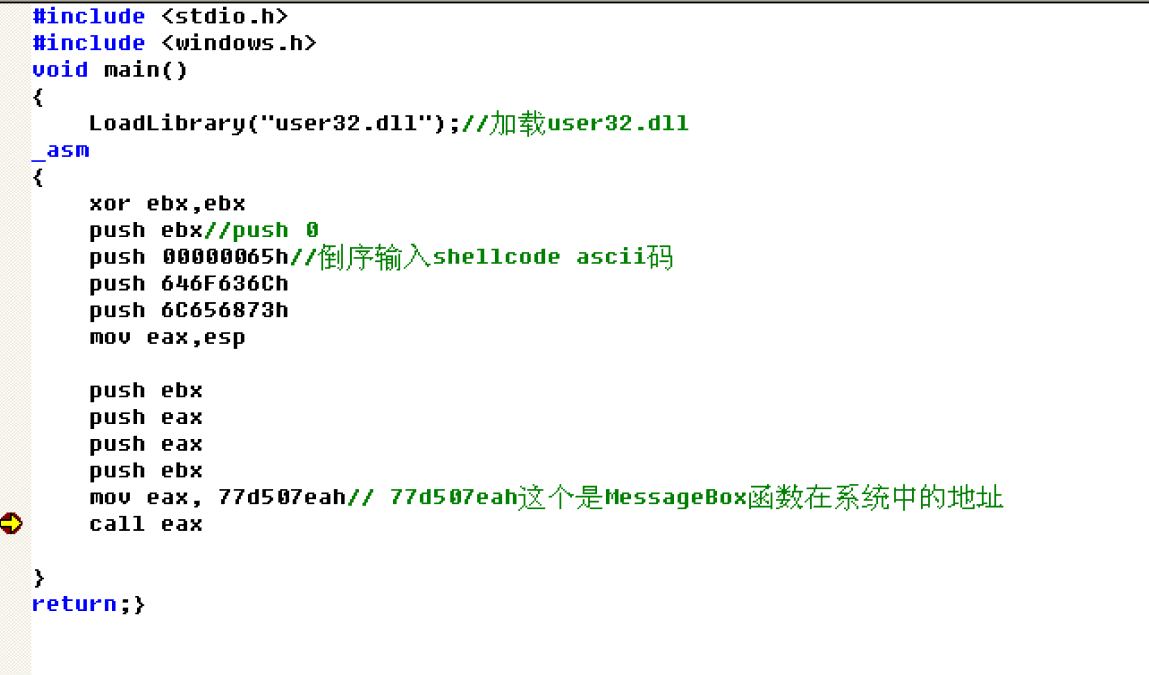
找到其对应汇编代码(Go to Disembly)



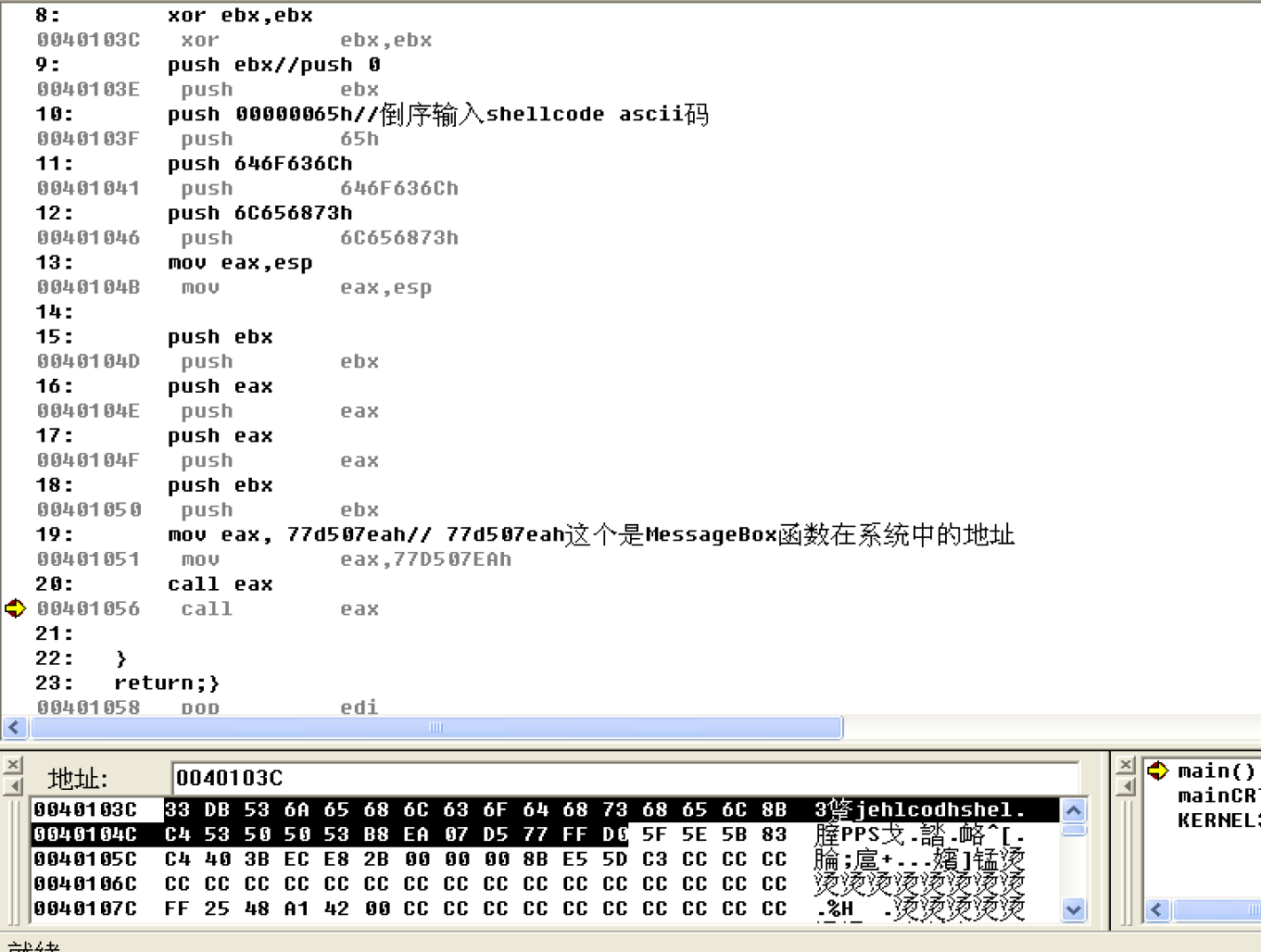


“shellcode”对应ascii码如上。

第三步：换成相应的汇编代码。

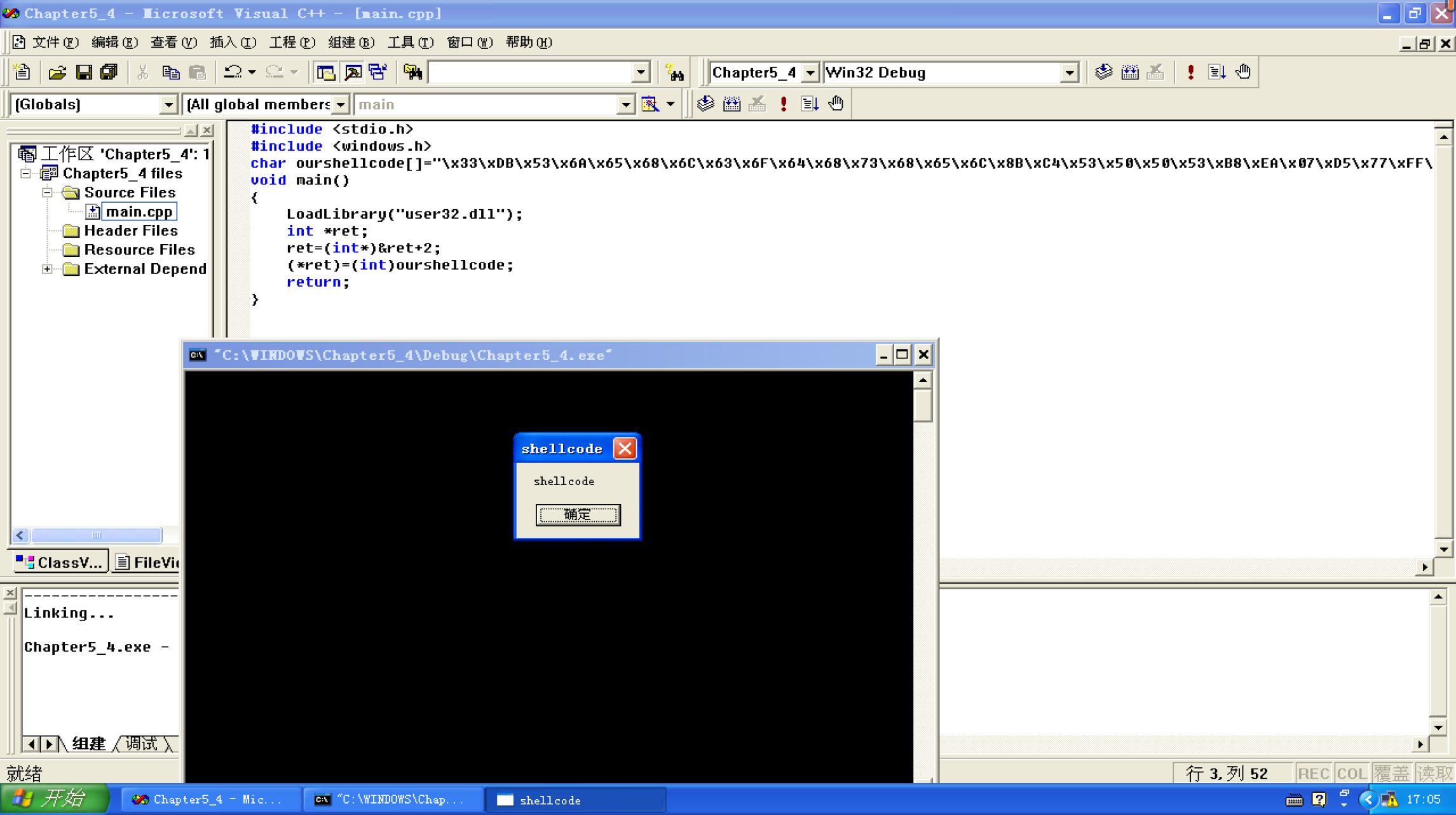


第四步：找到对应地址的机器码



\x33\xDB\x53\x6A\x65\x68\x6C\x63\x6F\x64\x68\x73\x68\x65\x6C\x8B\xC4\x53\x50\x50\x53\xB8\xEA\x07\xD5\x77\xFF\xD0

第五步：验证：



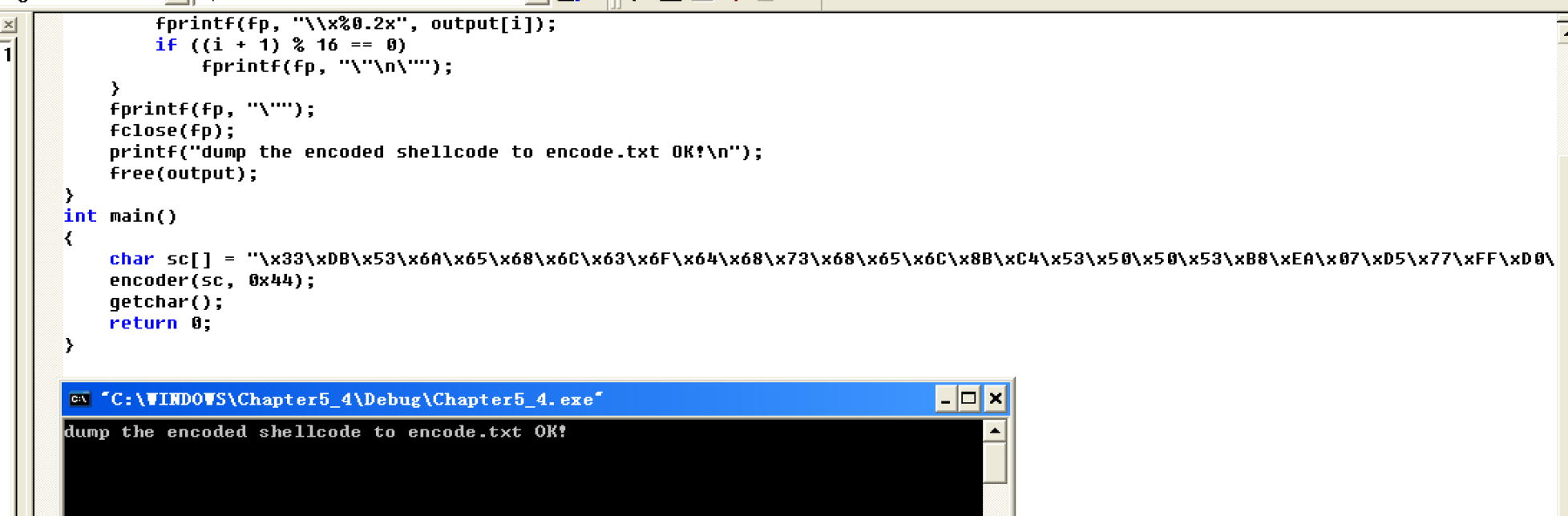
验证成功。

1. Shellcode编码原理

**异或编码**是一种简单易用的shellcode编码方法，它的编解码程序非常简单。但是，它也存在很多限制，比如在选取编码字节时，不可与已有字节相同，否则会出现0。此外，还有一些自定义编解码方法被采用，包括简单加解密、alpha\_upper编码、计算编码等。

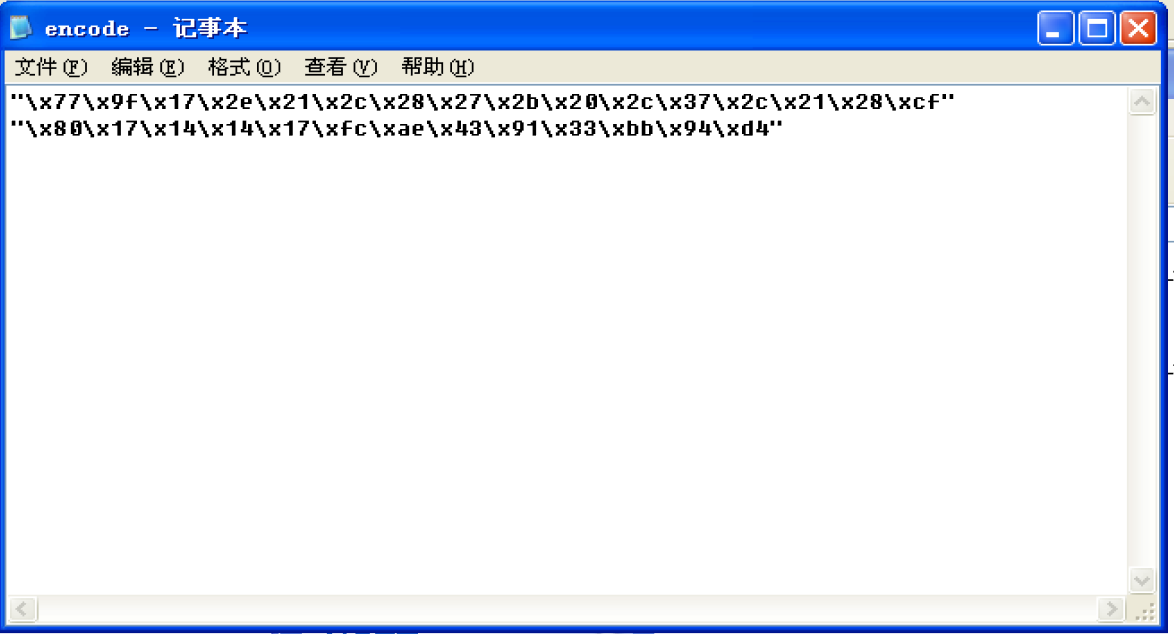
当exploit成功时，shellcode顶端的解码程序首先运行，它会在内存中将真正的shellcode还原成原来的样子，然后执行。这种对shellcode编码的方法和软件加壳的原理非常类似。这样，我们只需要专注于几条解码指令，使其符合限制条件就行，相对于直接关注于整段shellcode来说使问题简化了很多。

利用encoder()函数，将之前得到的‘shellcode’的Shellcode编码（末尾放一个空指令0x90作为结束符）作为参数，它的每一位与0x44进行异或运算，对Shellcode进行编码，将编码结果写入encode.txt中。



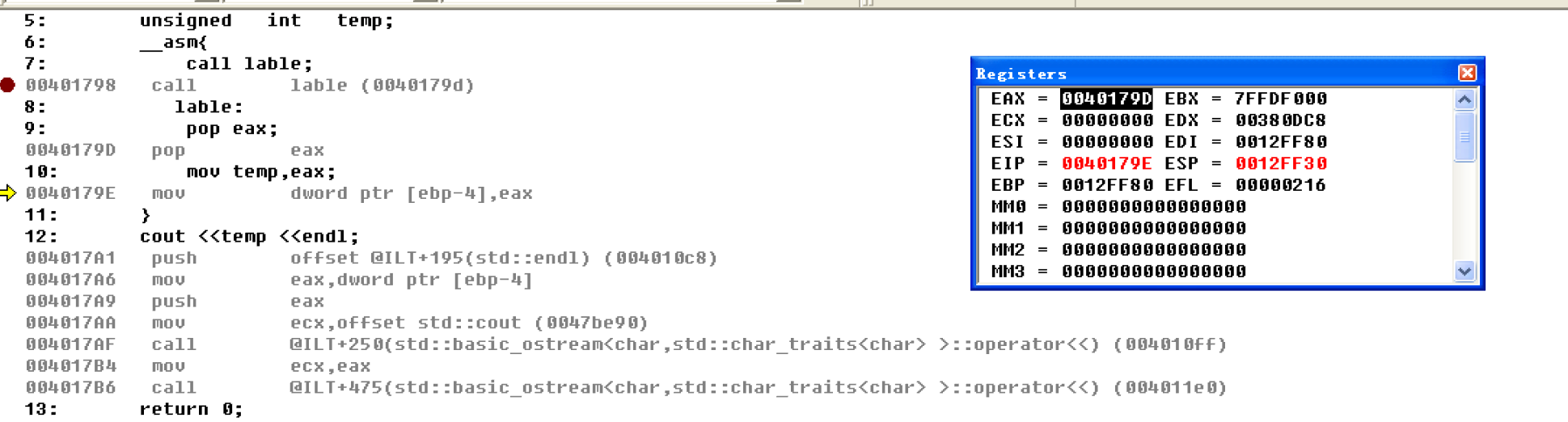
得到密码为：

"\x77\x9f\x17\x2e\x21\x2c\x28\x27\x2b\x20\x2c\x37\x2c\x21\x28\xcf\x80\x17\x14\x14\x17\xfc\xae\x43\x91\x33\xbb\x94\xd4"

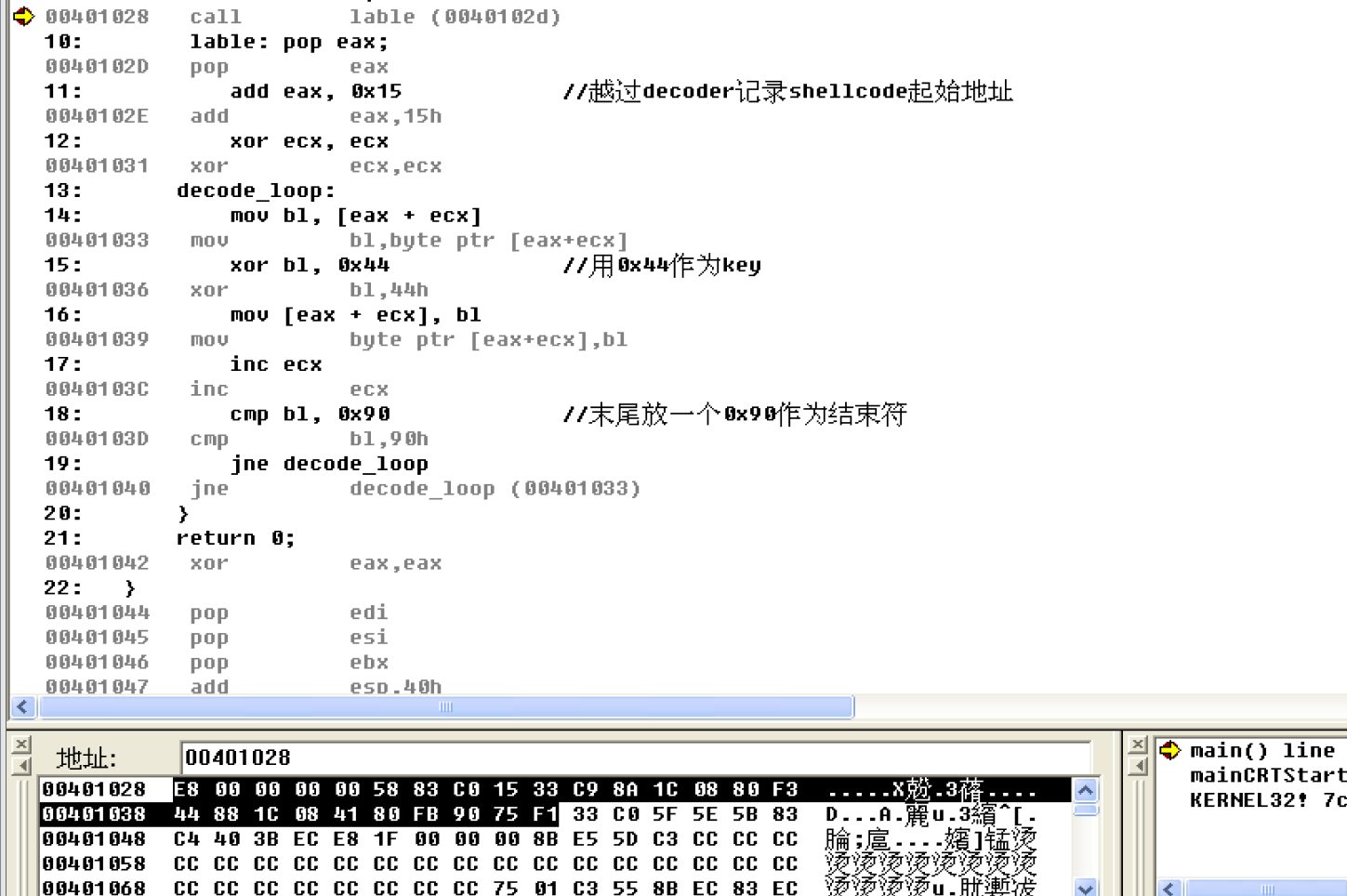


1. shellcode解码原理

call lable; lable: pop eax;”之后，eax的值就是当前指令地址了。原因是call lable的时候，会将当前EIP的值（也就是下一条指令pop eax的指令地址）入栈。因此，我们通过下面的程序来产生含有解码程序的Shellcode



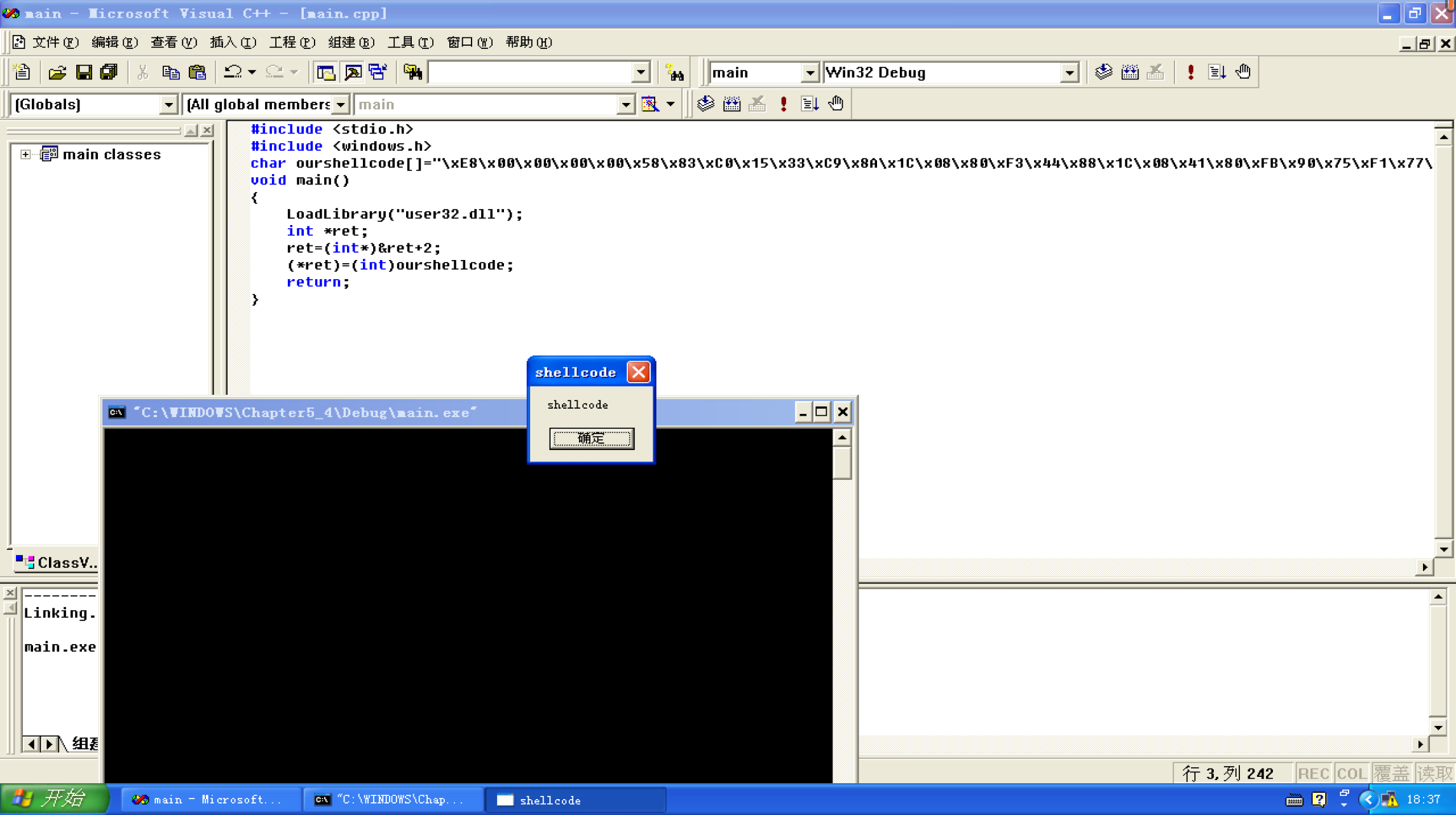
将每次把shellcode的代码异或特定key（0x44）后重新覆盖原先shellcode的代码。末尾，放一个空指令0x90作为结束符。再从call label语句的地址找到我们所要的答案：



即“\xE8\x00\x00\x00\x00\x58\x83\xC0\x15\x33\xC9\x8A\x1C\x08\x80\xF3\x44\x88\x1C\x08\x41\x80\xFB\x90\x75\xF1”.

再将其与之前调用MessageboxA输出“shellcode”的Shellcode的编码连接起来有：\xE8\x00\x00\x00\x00\x58\x83\xC0\x15\x33\xC9\x8A\x1C\x08\x80\xF3\x44\x88\x1C\x08\x41\x80\xFB\x90\x75\xF1\x77\x9f\x17\x2e\x21\x2c\x28\x27\x2b\x20\x2c\x37\x2c\x21\x28\xcf\x80\x17\x14\x14\x17\xfc\xae\x43\x91\x33\xbb\x94\xd4

再次测试结果为：



完成实验。

1. 总结

**shellcode编写思路：**

1. 装载动态链接库user32.dll

2）获得MessageBoxA函数的入口地址

3）c语言书写要执行的shellcode

4）找到其对应的汇编代码，进行加工，并写入项目中

5）根据汇编代码，找到对应地址中的机器码，编写shellcode

6）进行shellcode利用验证

**shellcode编码原理：**

对于二进制Shellcode机器代码的编码，通常采用类似“加壳”思想的手段，采用自定义编码的方法完成shellcode的编码，同时通过精心构造精简干练的解码程序，放在shellcode开始执行的地方，完成shellcode的编解码。

1. 在单独程序中编写编码代码，将原始shellcode进行异或编码。
2. 编写解码代码，先定位到shellcode起始位置（含解码代码），再向后偏移到执行shellcode的地方，将编码后的shellcode与原字符进行异或，实现解码。
3. 将上步的解码代码的机器码与编码后的shellcode进行链接，形成完整的shellcode代码
4. 进行shellcode利用验证

**心得体会：**

学习了shellcode的编码以及解码过程，对漏洞利用有了进一步了解。