《漏洞利用及渗透测试基础》实验报告

姓名：王亦辉 学号：2310764 班级：计科1班

**实验名称：**

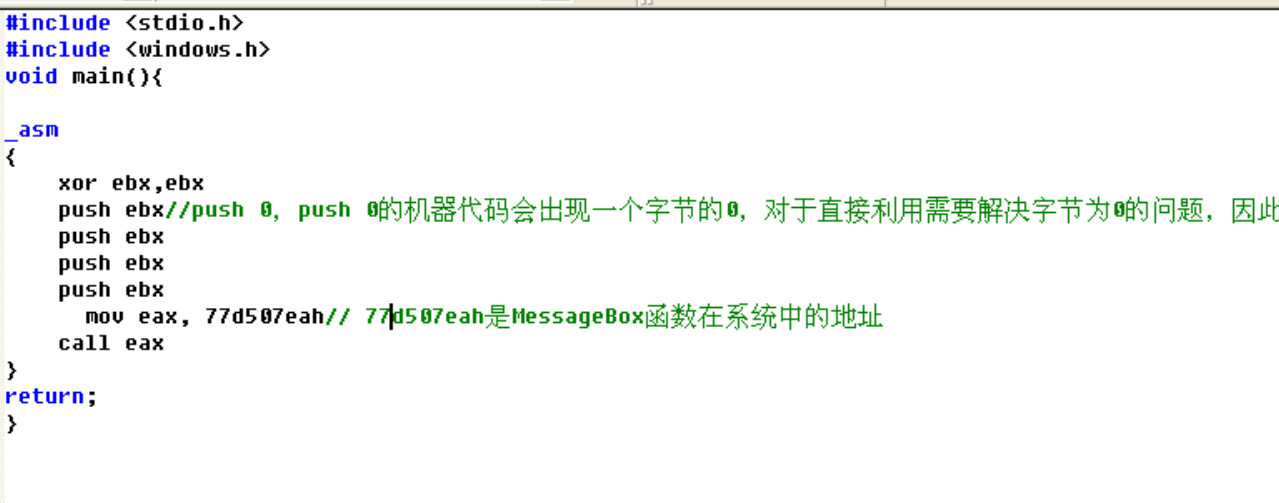
编写及提取shellcode代码

**实验要求：**

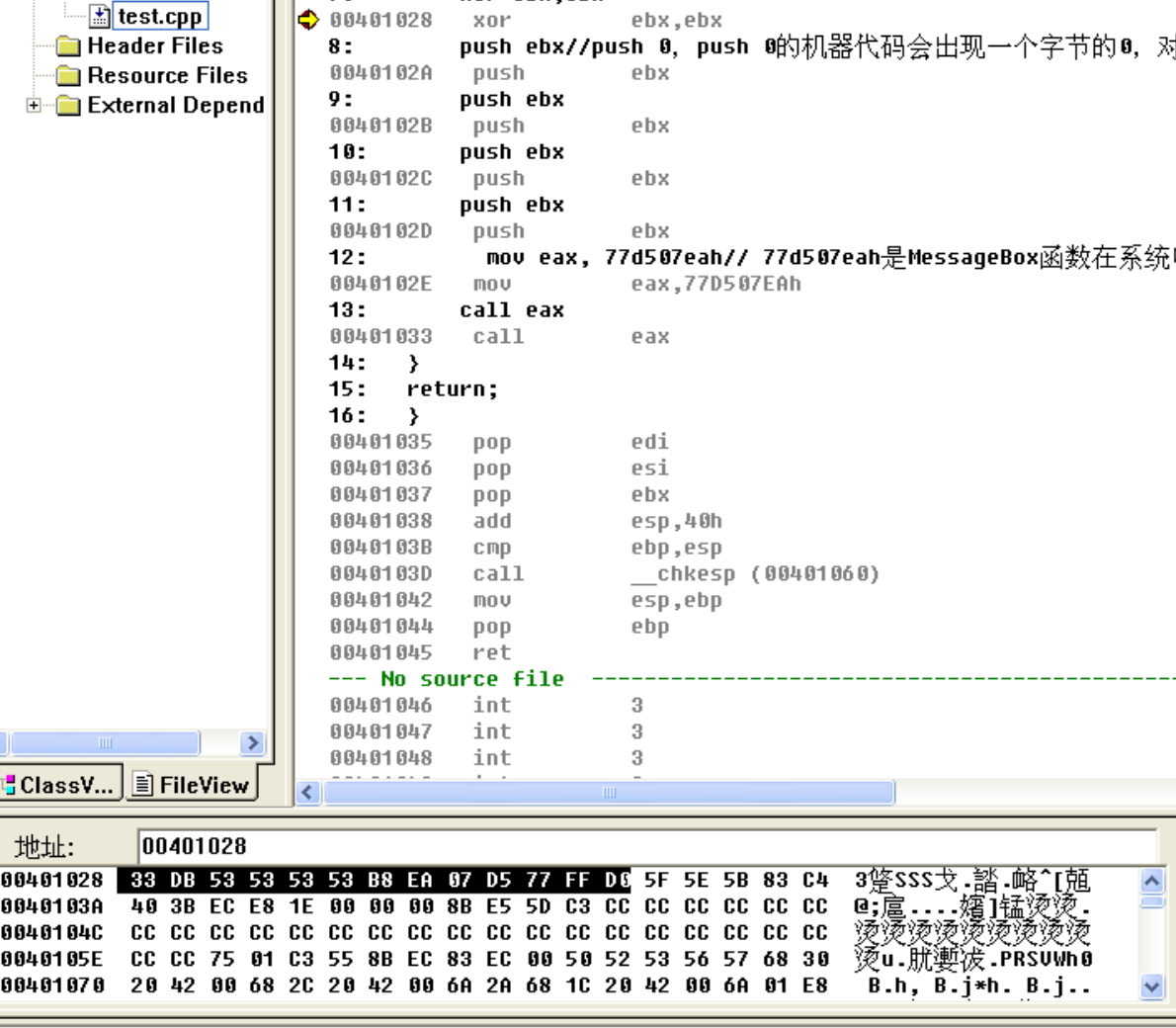
复现第五章实验三，并将产生的编码后的shellcode在示例5-4中进行验证，阐述shellcode编码的原理、shellcode提取的思想。

**实验过程：**

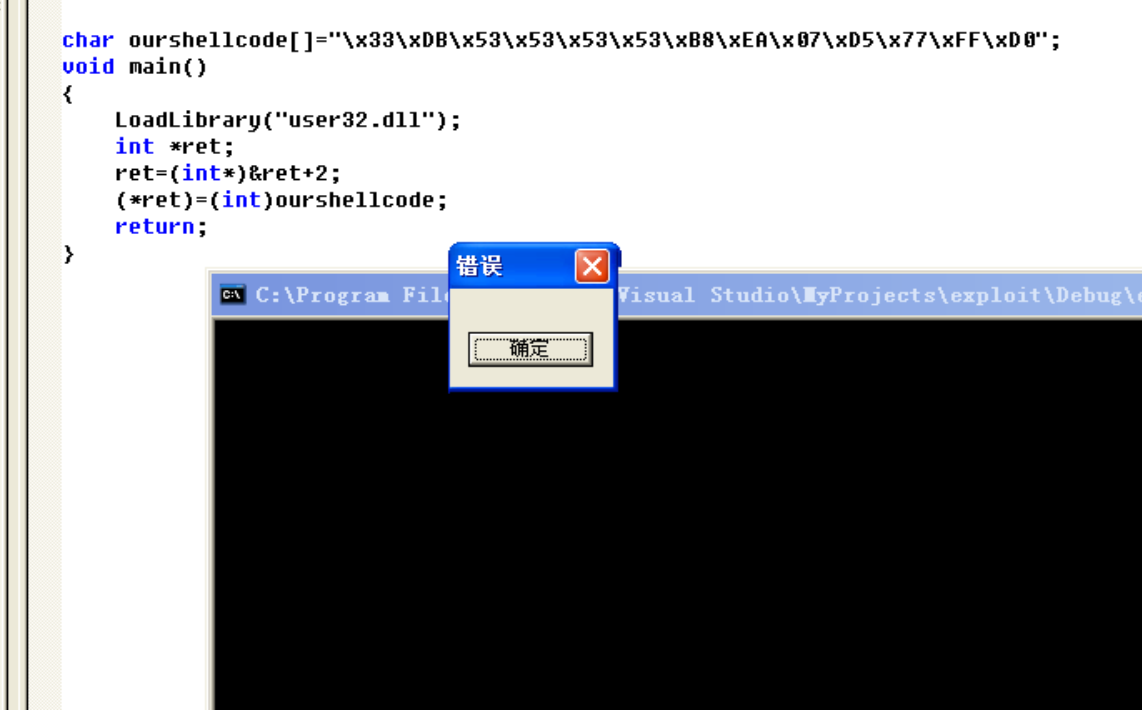
1. 首先直接用C写出程序，然后利用VC的反汇编功能得到汇编代码。（在这里我们直接得到了经过适当修改的汇编代码(push 0 改用xor实现) ）。



1. 将汇编代码反汇编，然后通过指令的地址，查看到我们汇编代码的机器码，这将是我们使用的shellcode。33 DB 53 53 53 53 B8 EA 07 D5 77 FF D0



1. 将此机器码的每个字节前面加上\x前缀，并且测试是否能调用对话框。发现有弹窗，通过栈溢出将程序控制权转移到此shellcode 后，它成功完成了弹出对话框的功能。



**心得体会：**

1. Shellcode 编码时，需要使用机器码，为了利用strcpy等函数，我们应该避免0x00 字节，因为这会被strcpy 认为是字符串的终止符。比如我们可以用xor 和push寄存器来代替push 0 。
2. Shellcode编码，比如使用xor编码，就是我们在存shellcode的功能部分的时候，是存机器码用xor转换之后的得到的字节们。在成功劫持到程序控制流之后，首先会运行shellcode的decoder部分，将shellcode还原成能够执行的代码，然后然后执行shellcode完成相应功能。
3. Shellcode提取，就是我们使用C语言把想要做的事情编写出来，然后进行反汇编，提取硬编码(机器码)，就得到了想要的shellcode，不过提取之后可能需要做一些修改才能使用。