《软件安全》实验报告

姓名：张丛 学号：2113662 班级：信安一班

**实验名称：**

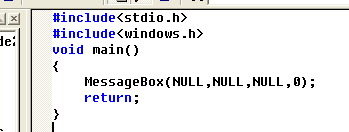
Shellcode编写及编码

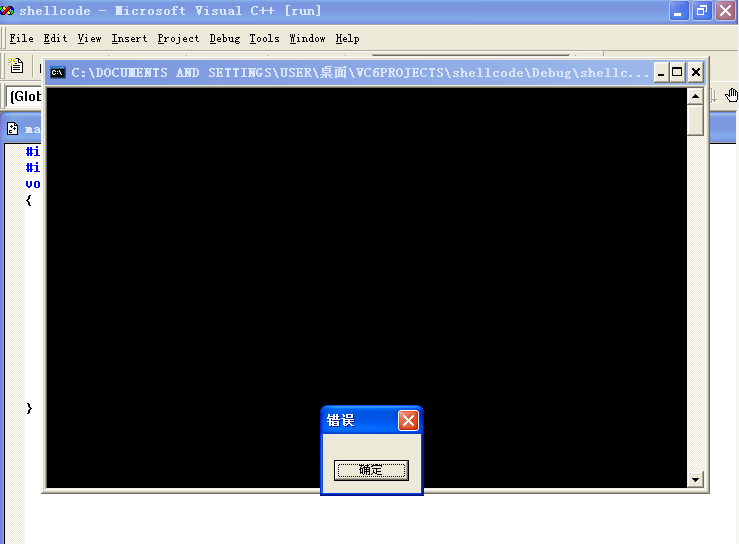
**实验要求：**

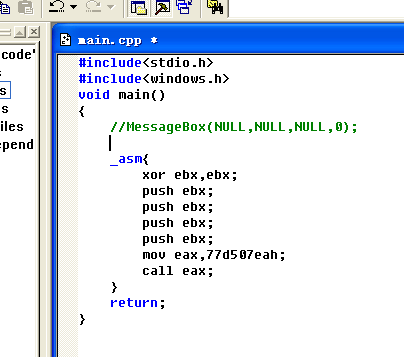
复现第五章实验三，并将产生的编码后的shellcode在示例5-4中进行验证，阐述shellcode编码的原理shellcode提取的思想。

**实验过程：**

1. 先写C的代码，知道大体结构，利用结构写汇编代码（如下图）

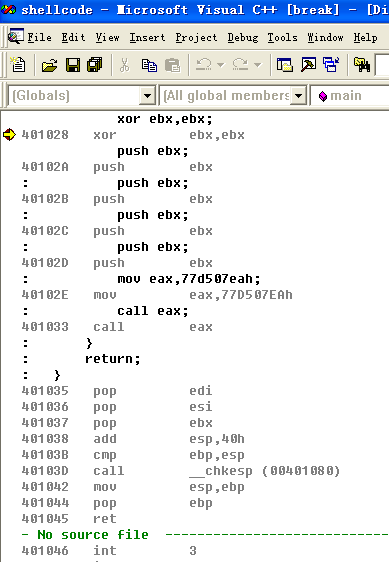




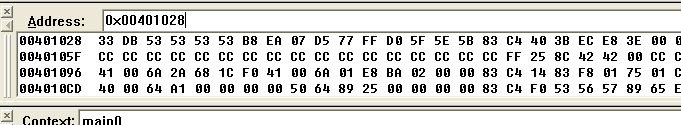


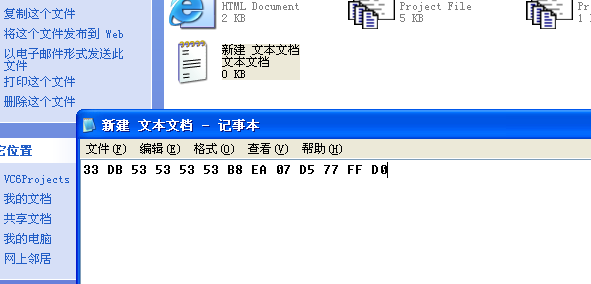
\_asm关键字可调用内联汇编程序。

2. 打断点，反汇编，看到代码逻辑

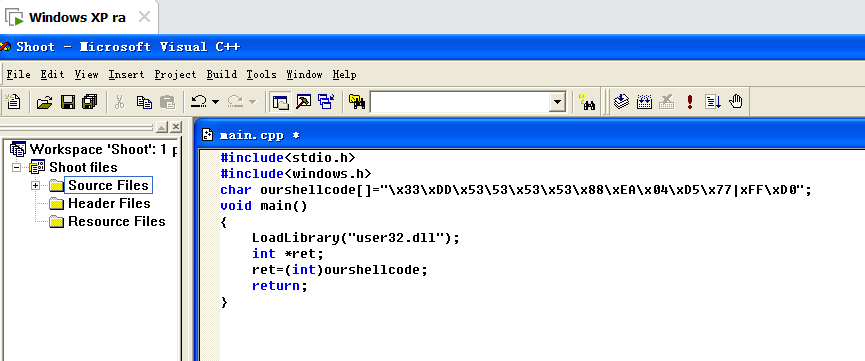


1. 查看保存机器码

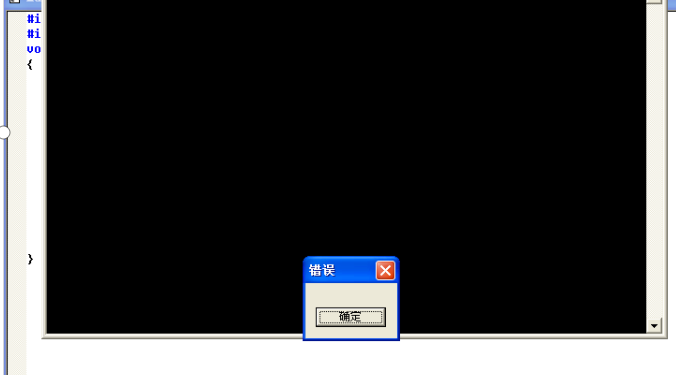




1. Shellcode代码植入



实验结果：



可见实现了shellcode代码的植入。

故整个实验完成了shellcode的编写及编码。

**心得体会：**

Shellcode编码原理：Shellcode实际是一段代码（也可以是填充数据），是用来发送到服务器利用特定漏洞的代码，一般可以获取权限。shellcode 的核心就是把代码写成 “与地址无关” 的风格，让它不论是在什么环境下都可以被执行。

Shellcode提取思想：主要是获得机器码，可通过汇编语言的编写来提取，汇编语言又可以利用高级语言获得。

这次实验主要复现了shellcode的编写编码以及植入。对shellcode相关的漏洞的理解加深，学习了编码shellcode的操作。