《软件安全》实验报告

姓名：曹瑜　　学号：2212794　　班级：密码科学与技术

实验名称：

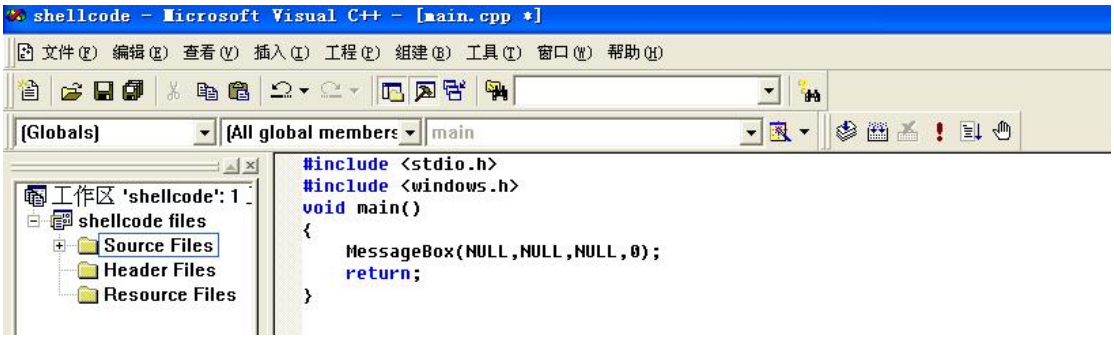
Shellcode 编写及编码实验

实验要求：

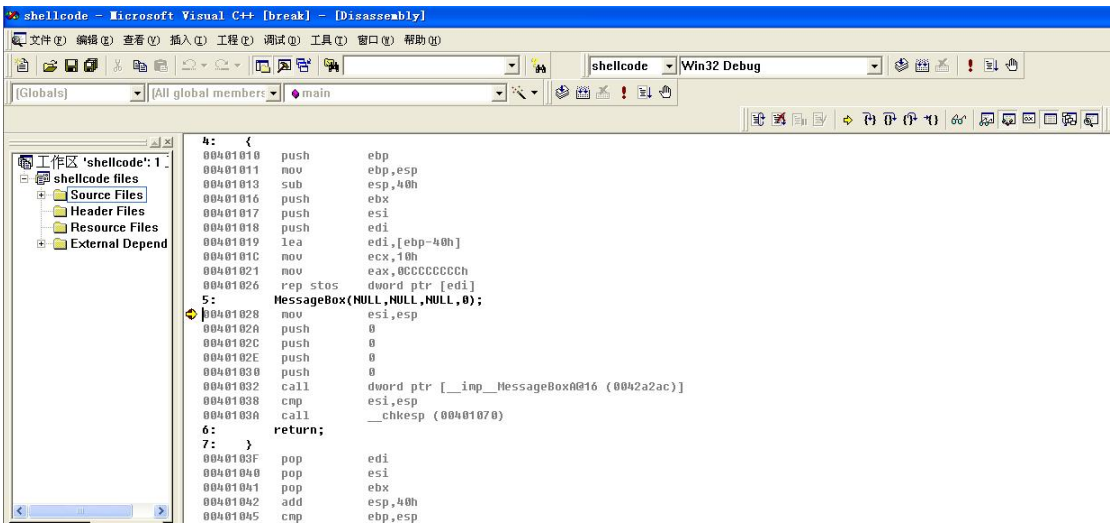
复现第五章实验三，并将产生的编码后的 shellcode 在示例 5-4 中进行验证，阐述 shellcode 编码的原理，shellcode 提取的思想

实验过程：

进入 VC：



进入 VC 反汇编可见代码逻辑：



更换成对应恶意汇编代码

```
#include <stdio.h>
#include <windows.h>
void main()
{
    _asm{
    xor ebx,ebx
    push ebx//push 0
    push ebx
    push ebx
    push ebx
     mov eax, 77d507eah// 77d507eah 这个是 MessageBox 函数在系统中的地址
    call eax

    }
    return;
}
```

转到起始句反汇编

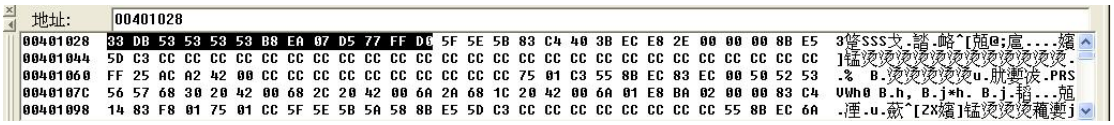
```
#include <stdio.h>
#include <windows.h>
void main()
{
    _asm{
    xor ebx,ebx
    push ebx//push 0
    push ebx
    push ebx
    push ebx
     mov eax, 77d507eah// 77d507eah 这个是 MessageBox 函数在系统中的地址
    call eax

    }
    return;
}
```

```
00401028   xor         ebx,ebx
7:        push ebx//push 0
0040102A   push        ebx
8:        push ebx
0040102B   push        ebx
9:        push ebx
0040102C   push        ebx
10:       push ebx
0040102D   push        ebx
11:        mov eax, 77d507eah// 77d507eah 这个是 MessageBox 函数在系统中的地址
0040102E   mov         eax,77D507EAh
12:       call eax
00401033   call        eax
13:
14:       }
15:       return;
16:   }
00401035   pop         edi
```

转到对应区域地址，可见该部分指令从地址 00401028 到 00401034 处

根据地址可定位到对应的机器码



新建文本存储对应机器码

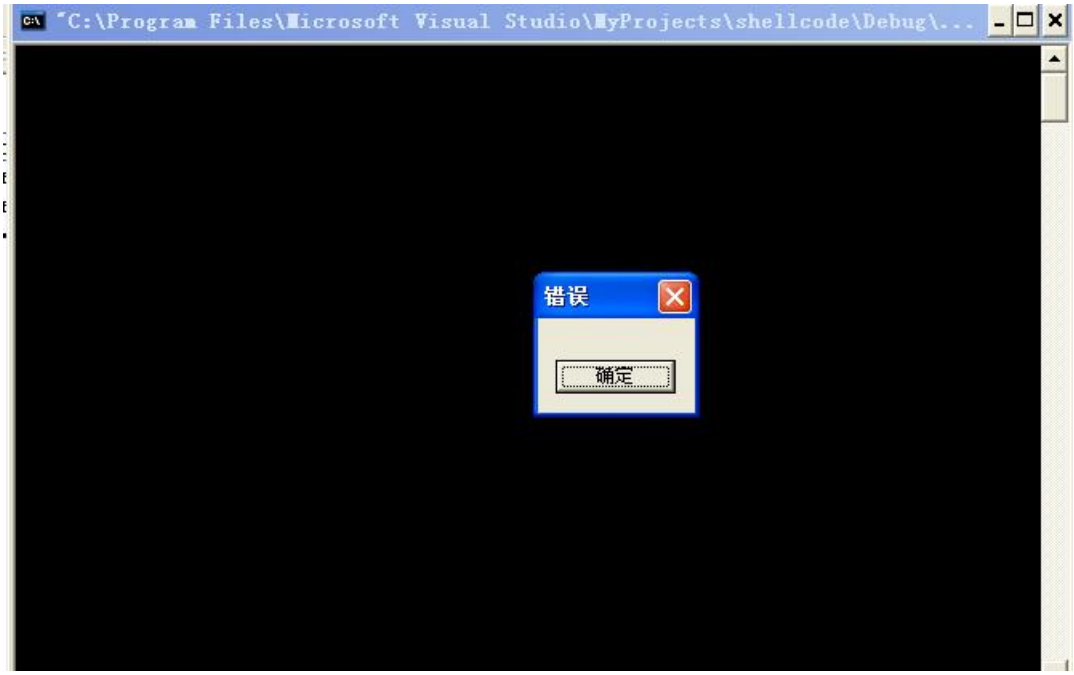
利用该 shellcode 实现漏洞利用，编写调试程序验证：

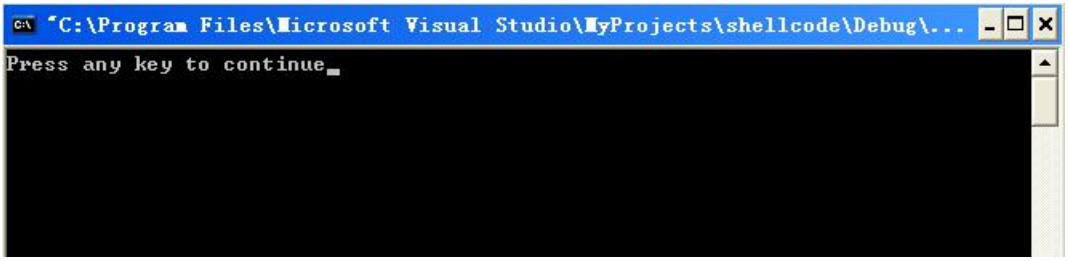
```
#include <stdio.h>
#include <windows.h>
char ourshellcode[]="\x33\xDB\x53\x53\x53\x53\xB8\xEA\x07\xD5\x77\xFF\xD0";
void main()
{
    LoadLibrary("user32.dll");
    int *ret;
    ret=(int*)&ret+2;
    (*ret)=(int)ourshellcode;
    return;
}sS
```

处理所得机器码

运行程序可得知该 shellcode 可以调用 MessageBox

```
#include <stdio.h>
#include <windows.h>
char ourshellcode[]="\x33\xDB\x53\x53\x53\x53\xB8\xEA\x07\xD5\x77\xFF\xD0";
void main()
{
    LoadLibrary("user32.dll");
    int *ret;
    ret=(int*)&ret+2;
    (*ret)=(int)ourshellcode;
    return;
}sS
```





心得体会：

通过本次实验，掌握了如何根据汇编代码，找到对应地址的机器码，对 shellcode 进行编码和解码操作。通过本次实验，基于理论知识的学习初次尝试了 shellcode 的提取和调试，对 shellcode 的提取和编译有了更深入的了解。