《软件安全》实验报告

姓名： 邢清画 学号： 2211999 班级：1023

**实验名称：**

Shellcode编写及编码

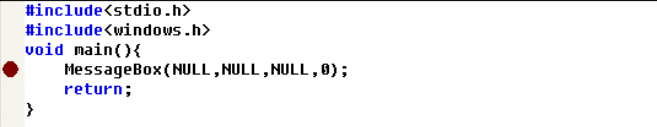
**实验要求：**

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. 用C语言编写要执行的shellcode

代码如下：



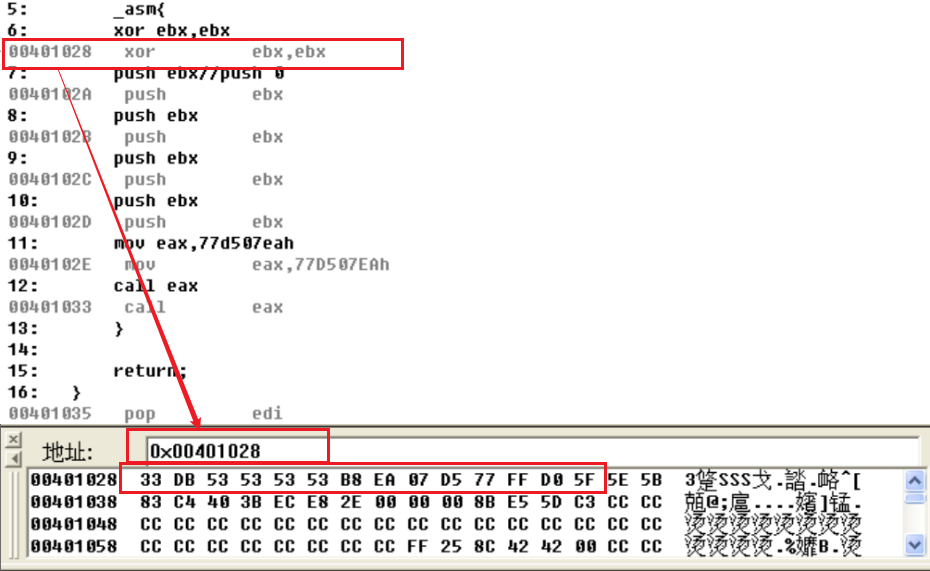
在MessageBox(NULL,NULL,NULL,0);处设置断点，进入反汇编模式，观察该函数在调用时的反汇编代码，共调用了四个参数，如下：



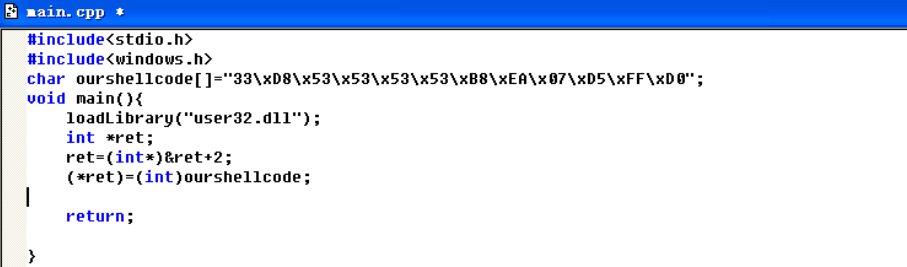
在编译器中使用\_asm编写MessageBox 的反汇编语句：

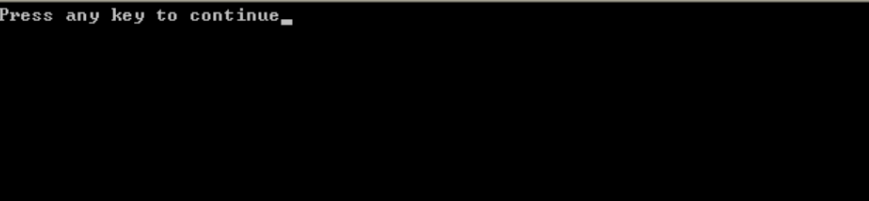
正确运行后，证明该代码的功能与上述MessageBox 函数相同。

在xor ebx,ebx语句处加入断点，进入反汇编



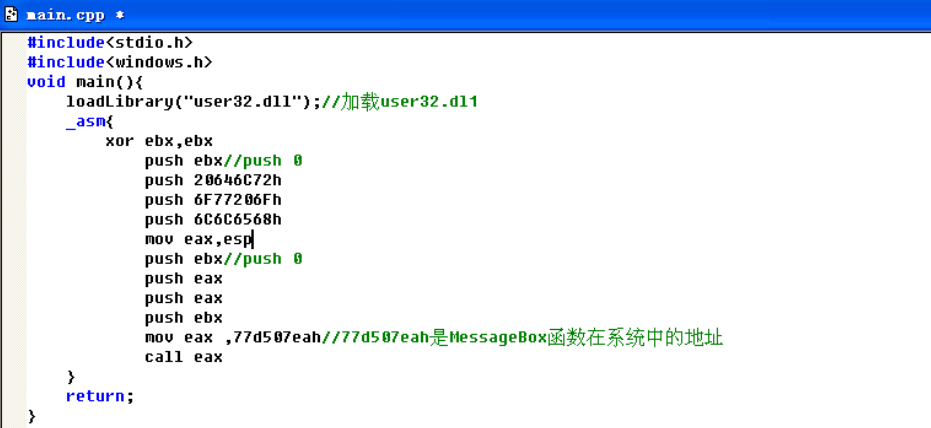
根据汇编语句的地址，获得该汇编语句对应的机器码，并在shellcode处替换进行调试





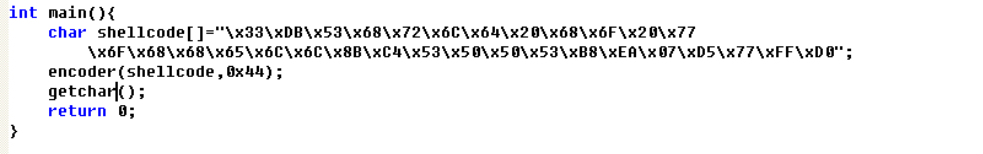
1. 编写shellcode:

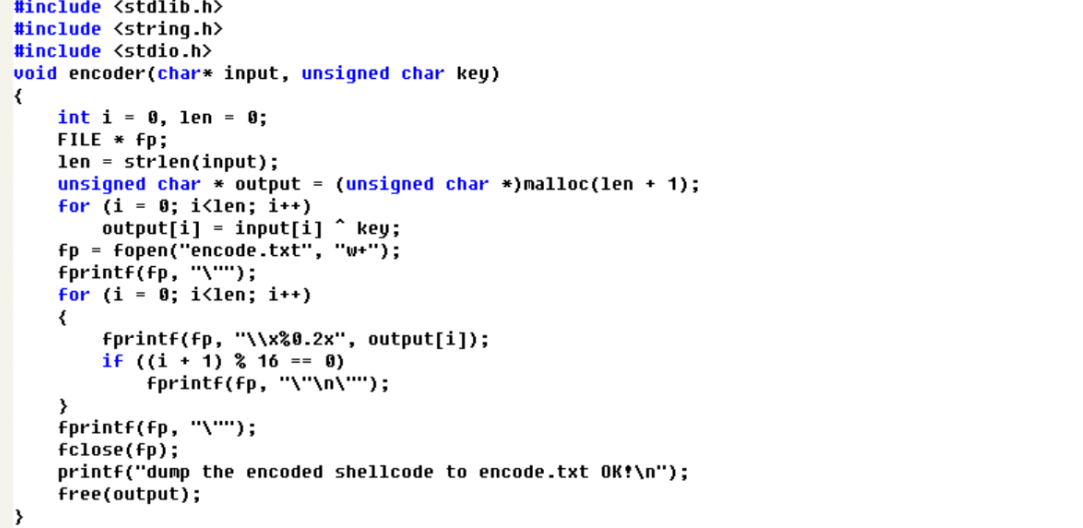
实现可以输出“hello world”的运行框，代码如下：

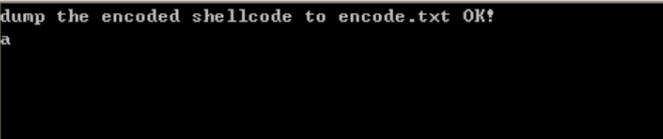


提取shellcode代码：\x33\xDB\x53\x68\x72\x6C\x64\x20\x68\x6F\x20\x77\x6F\x68\x68\x65\x6C\x6C\x8B\xC4\x53\x50\x50\x53\xB8\xEA\x07\xD5\x77\xFF\xD0

1. shellcode编码：

用异或编码，输入得到的shellcode代码，代码如下：

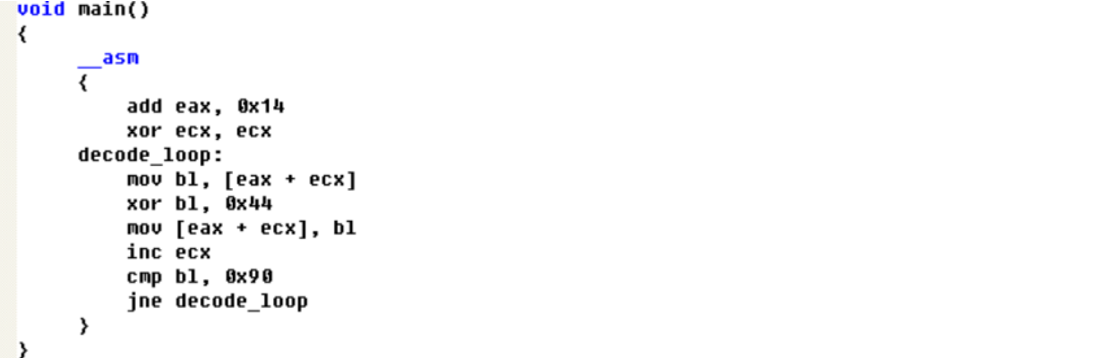




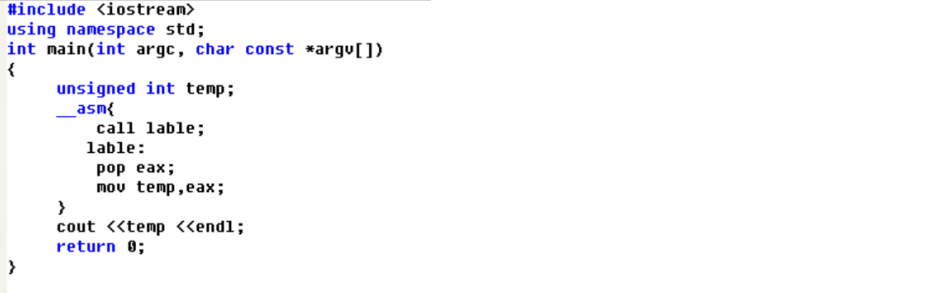
并输出异或操作之后的shellcode编码到encode.txt中，获得编码后的shellcode:



1. shellcode解码操作：

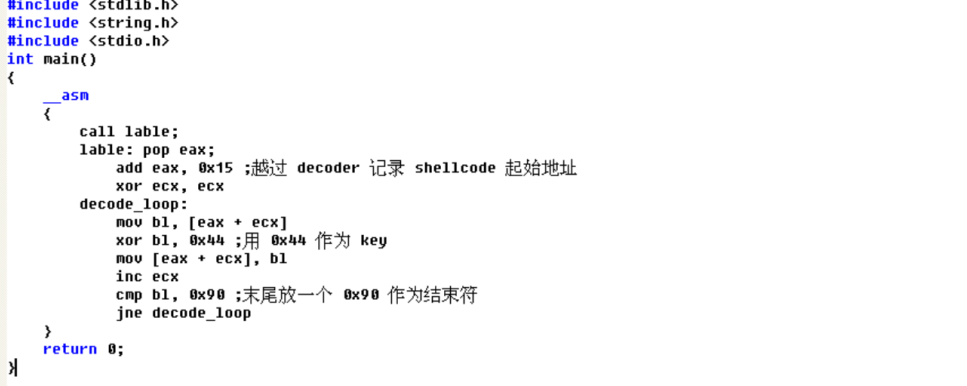
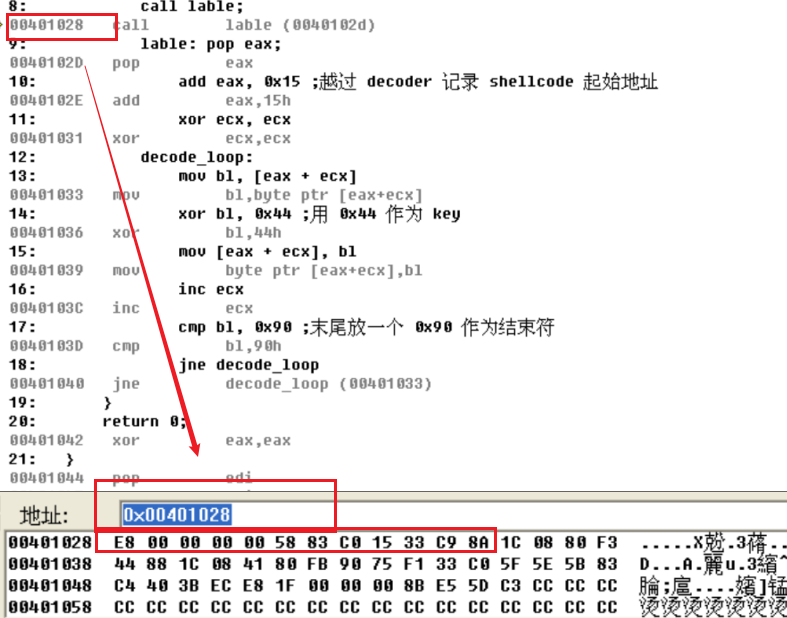
解码代码如下：  


解码器与编码后的shellcode共同执行，以eax作为shellcode的起始地址，在之后的每次操作中，将代码和0x44做异或操作后覆盖掉之前的代码，在最后放置0x90为结束符。



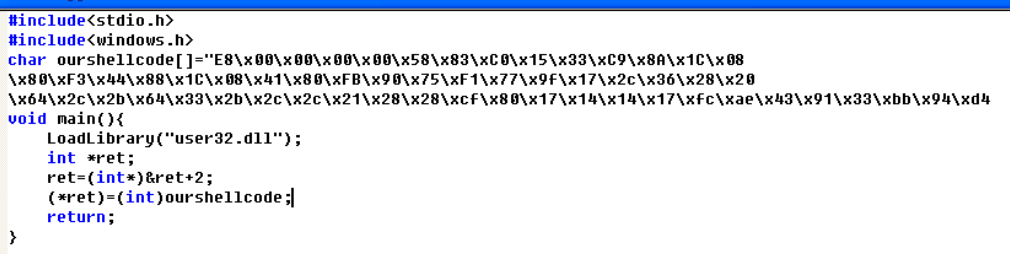
进入反汇编代码部分：  


观察到在执行完call lable语句之后，将eip存储的下一条指令地址的值（0040157d）压入栈，eax是当前的指令地址。

编写并执行下面的程序代码：  
产生含有解码程序的shellcode，进入反汇编部分：

根据汇编语句的地址（00401028），获得该汇编语句对应的机器码。从开始地址不断提取机器码。00401042处为结束地址，在提取到00401041时，与encode.txt中的shellcode编码合并得到完整的shellcode编码：

E8\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\x2c\x36\x28\x20\x64\x2c\x2b\x64\x33\x2b\x2c\x2c\x21\x28\x28\xcf\x80\x17\x14\x14\x17\xfc\xae\x43\x91\x33\xbb\x94\xd4

在示例5-4中代替ourshellcode具体值：  


编译运行：



**心得体会：**

通过根据实验案例，编写代码实现了shellcode的编码和解码过程，并了解了内在原理。Shell是命令解释器，用于解释输入的命令，植入shell的代码是shellcode，用来表示广义上的植入进程的代码，它是指一段与操作系统交互的机器码,通常编写用于利用软件漏洞或执行恶意代码的目的，是用来利用计算机系统弱点的攻击手段之一。通过了解攻击过程，更好的防止恶意代码攻击。