《软件安全》实验报告

姓名：胡博浩 学号：2212998 班级：信息安全

**实验名称：**

OLLYDBG软件破解

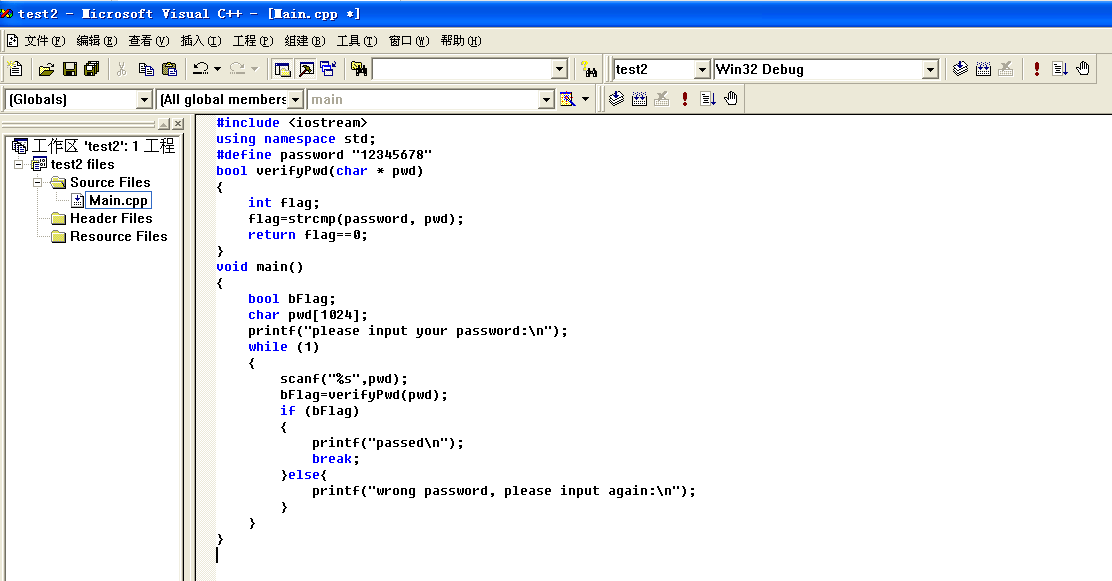
**实验要求：**

1. 请在XP VC6生成课本第三章软件破解案例（DEBUG模式，示例3-1）。进而使用OllyDBG进行单步调试，获取verifyPWD函数对应flag==0的汇编代码，并对这些汇编代码进行解释。
2. 对生成的DEBUG程序进行破解，复现课本上提供的两种破解方法。

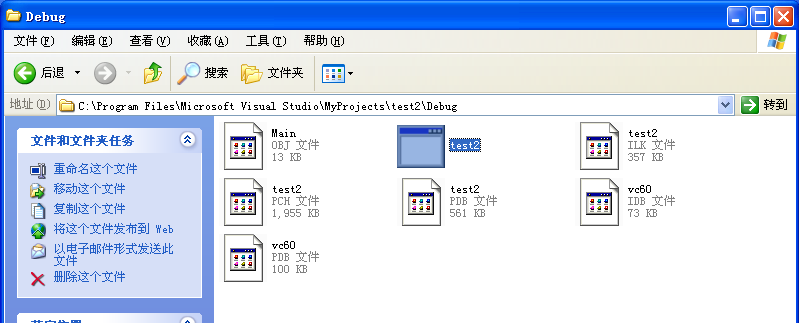
**实验过程：**

一、生成exe文件

1.创建新项目，并编写代码

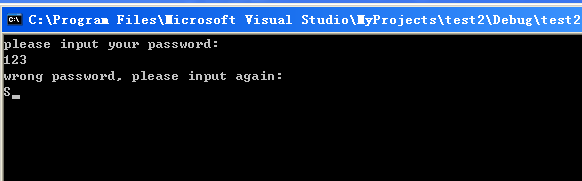


2.编译链接形成exe文件

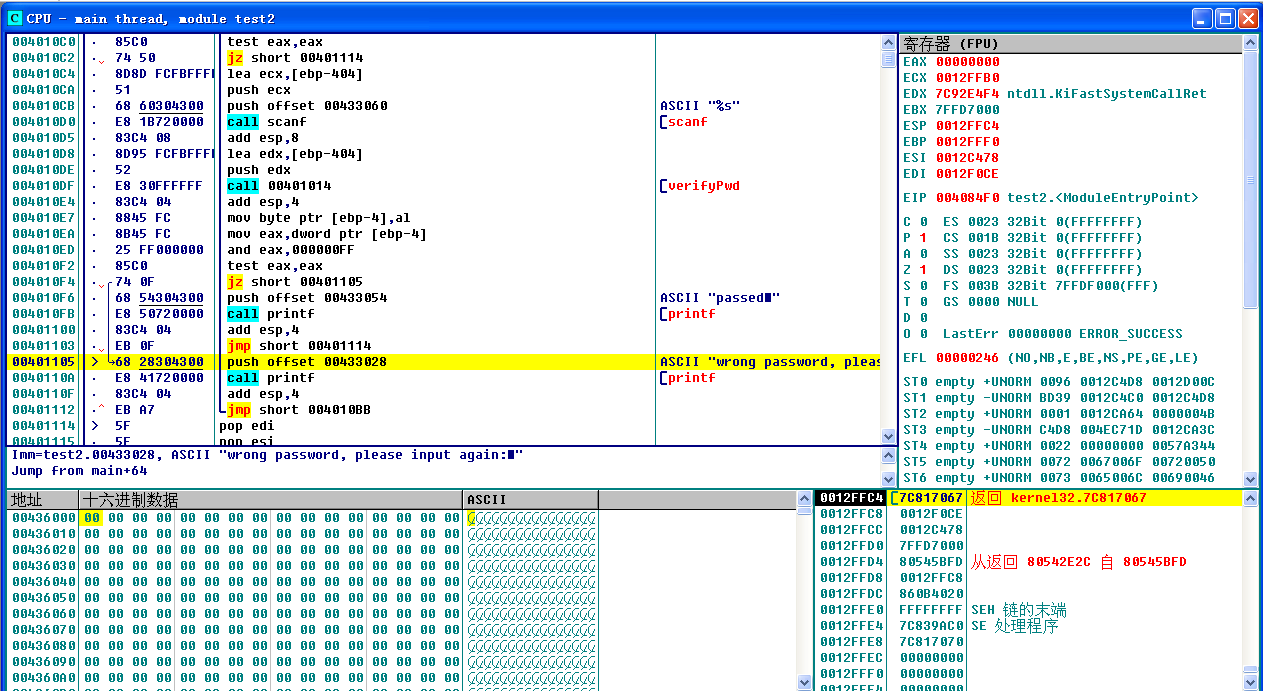


二、使用OllyDBG进行单步调试，获取verifyPWD函数对应flag==0的汇编代码

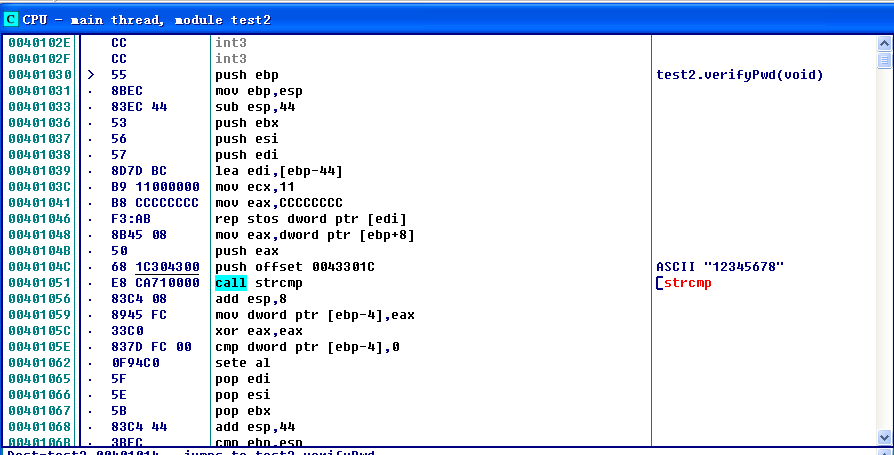
1.运行程序，获取提示信息“wrong”



2.用ollyDBG打开，通过OllyDBG的字符串查找功能，定位wrong字符串的位置



3. 向上发现call 00401014，即调用verifyPwd函数，随便输入123，然F7步入，即可看到verifyPWD函数的调用过程。



4.对于函数中的代码：

flag=strcmp(password, pwd);

return flag==0;

被解释为汇编语言：

Mov dword ptr [ebp-4], eax //将strcmp函数调用后的返回值（存在eax中）赋值给变量flag

Xor eax, eax //将eax的值清空

Cmp dword ptr [ebp-4], 0 //将flag的值与0进行比较，即flag==0;

Sete al //在flag等于0时，将al设置为1，否则默认为0

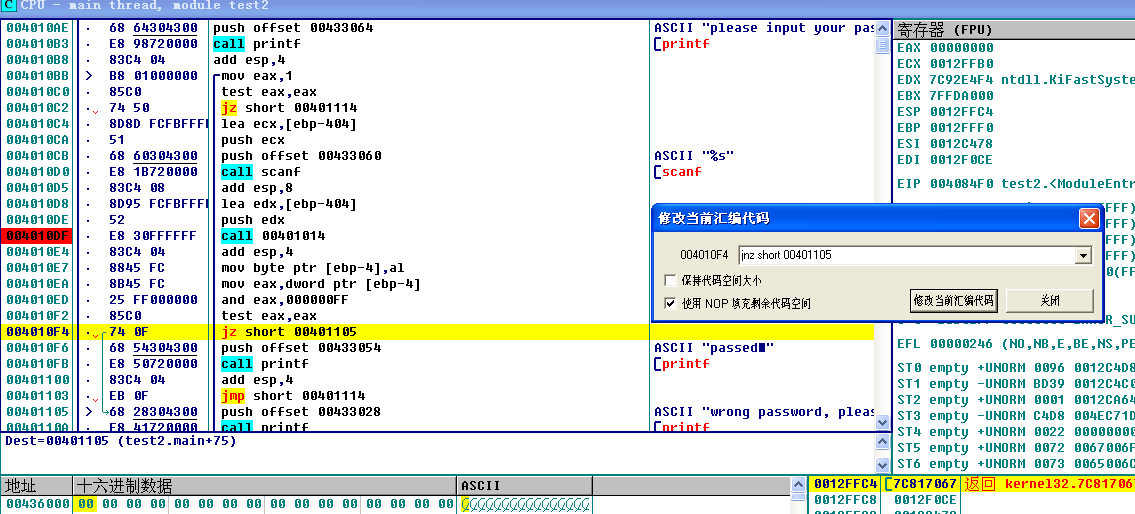
三、对生成的DEBUG程序进行破解

1.方法一：修改关键跳转指令

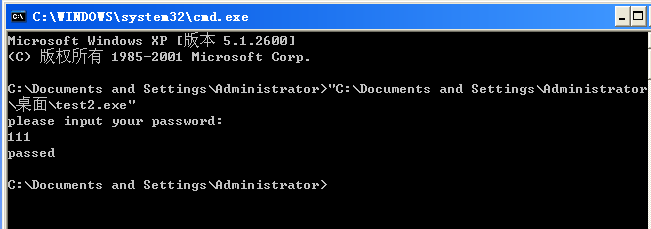
Test eax, eax

Jz short 0041364b

1. 这两行汇编代码是实现判断跳转的关键逻辑。将jz改为jnz，即可使大概率的密码错误事件将会正常跳转到验证正确的部分，而密码正确时的小概率事件则会显示密码错误。

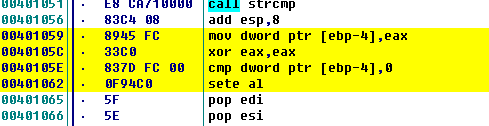


（2）修改后错误密码会通过

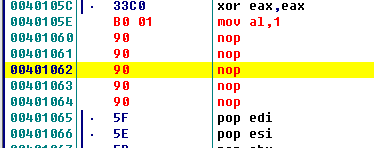


2.方法二：修改函数返回值

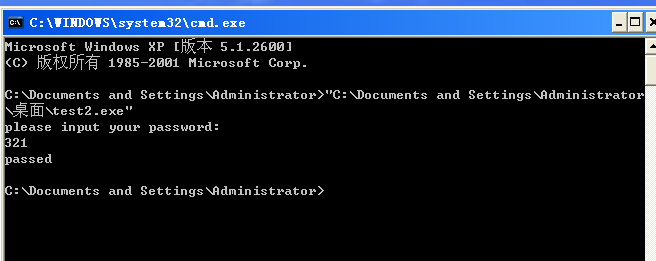
（1）思路是修改verifyPwd函数，使其返回的恒为真值。



（2）将cmp指令修改为mov指令，强行将eax中的值设置为1，同时为了能够消除sete的意外影响，我们将其nop掉。



（3）同样生成新的可执行文件，运行后发现无论输入什么密码，均能通过。



**心得体会：**

1. 通过本次实验，我深刻认识到了OllyDBG这一强大的调试工具的重要性，并通过实践掌握了其基本用法。我学会了如何利用OllyDBG进行动态调试，设置断点、监视寄存器以及查看内存等功能，这为我后续的逆向分析和破解工作提供了强大的支持。
2. 同时，我也在实验中掌握了通过修改指令来实现软件破解的技巧。通过分析和修改汇编代码，我能够改变程序的行为，绕过或者修改软件的限制，这对于安全领域的研究和实践具有极大的意义。

3.此外，本次实验也让我重新巩固了对汇编代码的知识。通过实践分析和修改汇编代码，我更深入地理解了计算机程序的底层原理，加深了对汇编语言的理解。