《软件安全》实验报告

姓名：蒋薇　　学号：2110957　　班级：计科 1 班

实验名称：

软件破解

实验要求：

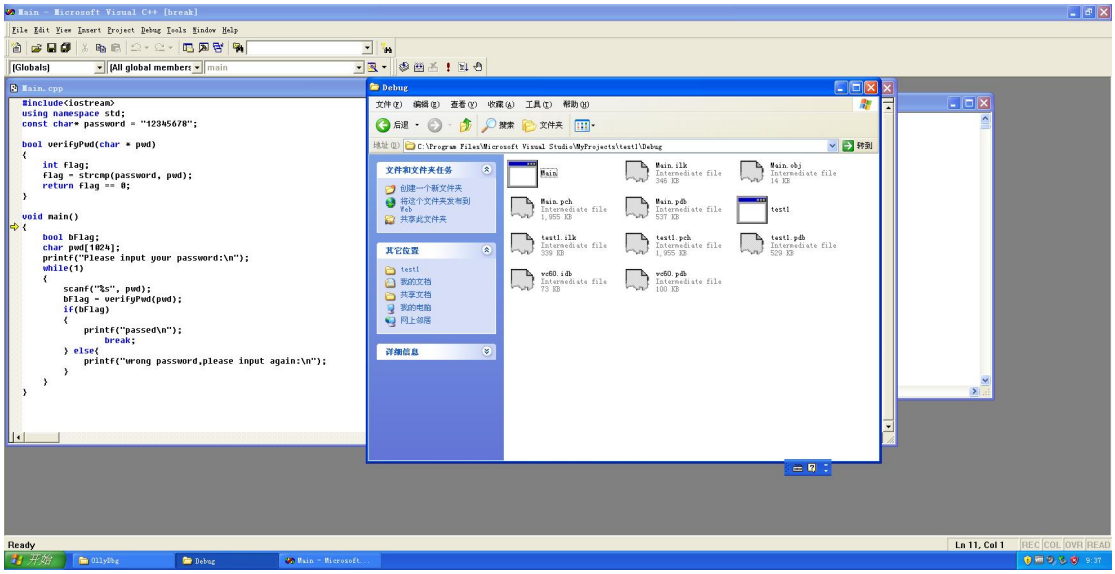
1. 在 XP VC6 生成课本第三章软件破解的案例(DEBUG 模式，示例 3-1)
2. 使用 OllyDBG 进行单步调试，获取 verifyPWD 函数对应 flag==0 的汇编代码，并对这些汇编代码进行解释。
3. 对生成的 DEBUG 程序进行破解，

（1）复现课本上提供的两种破解方法 1

（2）破解方法 2

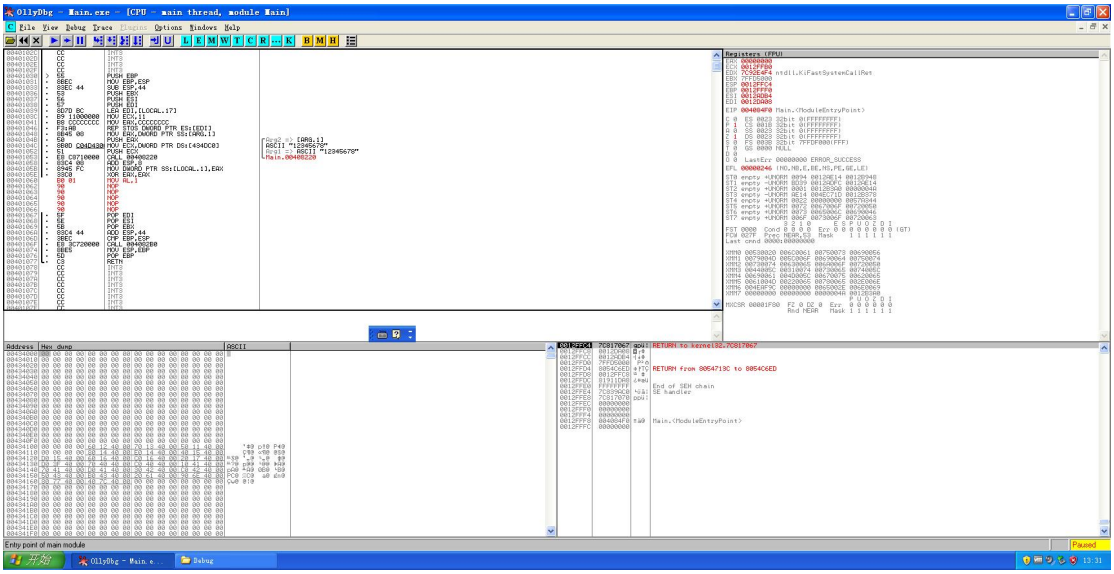
实验过程：

1. 在 XP VC6 生成课本第三章软件破解的案例(DEBUG 模式，示例 3-1)，即将实例 3-1 源代码生成的 Debug 模式的可执行文件，使用 OllyDBG 进行破解



破解目标：输入任意，都可通过

2. 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。



ebp 指针入栈，ebp 向上走，设为 esp 的值，esp 减 44h,开辟空间进行接下来处理，
相关指针入栈 ebx,esi,edi,ecx 记录循环，填充 CCh,
xor 异或处理，相同置 0，相反置 1
使用 eax 寄存器，必有返回值处理，本代码中返回值为 bool 类型，使用 sete al，影响状态位，
Pop()相关指令，retn，后 esp，ebp 回到原来位置

3 对生成的 DEBUG 程序进行破解，

（1）现课本上提供的两种破解方法 1

输入错误的，跳到正确的逻辑处执行

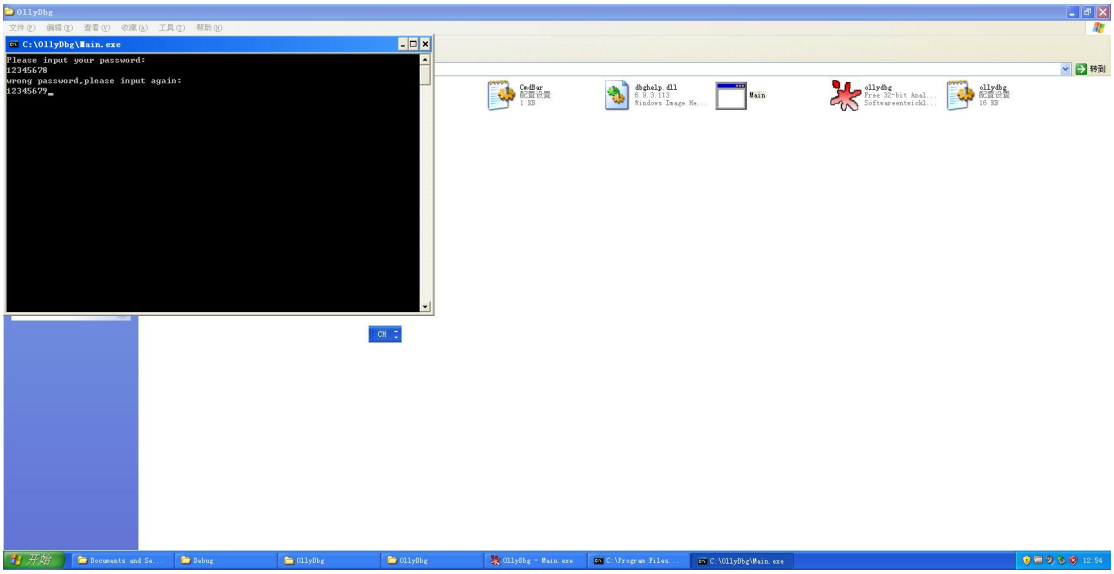
破解有利信息，错误时的输出“wrong password”处，

查找-->查找所有引用的字符串（ctrl+F）->双击

发现输出“Wrong”提示前有跳转指令，满足即跳转

做法：取反，jz->jnz,破坏逻辑，双击修改，保持空间大小，后逻辑变为：错误输入-》原正确逻辑，正确输入-》原错误逻辑;

编辑-->复制所有修改到可执行文件，保存文件成可执行文件，截图如下：



（2）两种破解方法 2

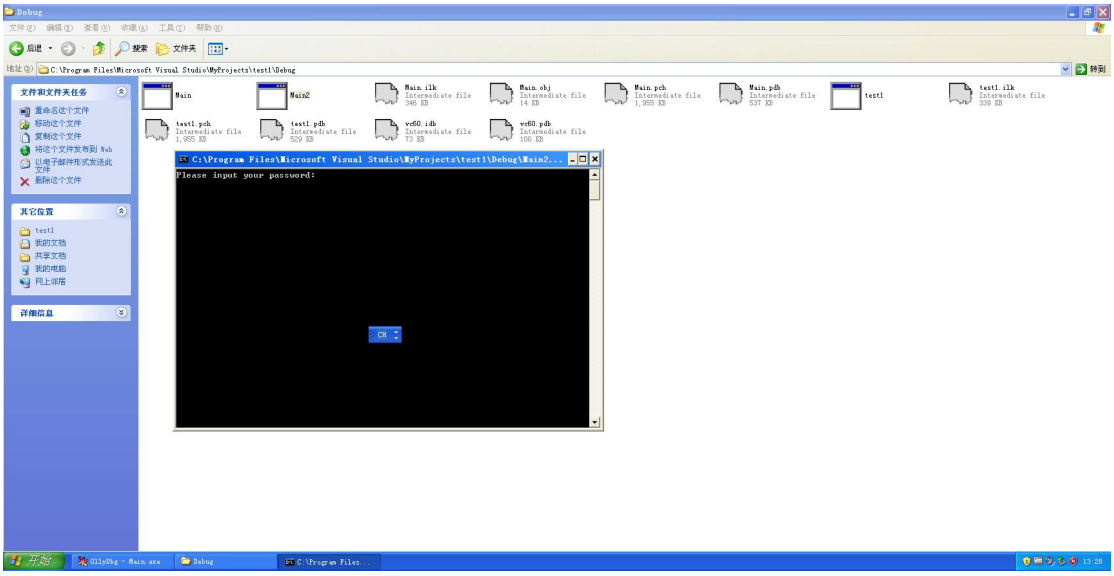
无论输入对错，强制控制返回值，劫持控制流，程序总是转入正确逻辑处

通过跟随条件转移前的 call 调用，转到函数中，

Retn 返回前，必有返回值处理，本代码中返回值为 bool 类型，使用 sete al，影响状态位，

分析：无论是否比较，强制更改 al,cmp()函数，

做法： 双击--》不保存代码空间大小--》mov al，01， sete al,--> nop,编辑、保存



心得体会：

通过实验，掌握了通过汇编代码理解代码逻辑，在理解逻辑基础上，通过修改相关代码，实现我的目的