《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：**

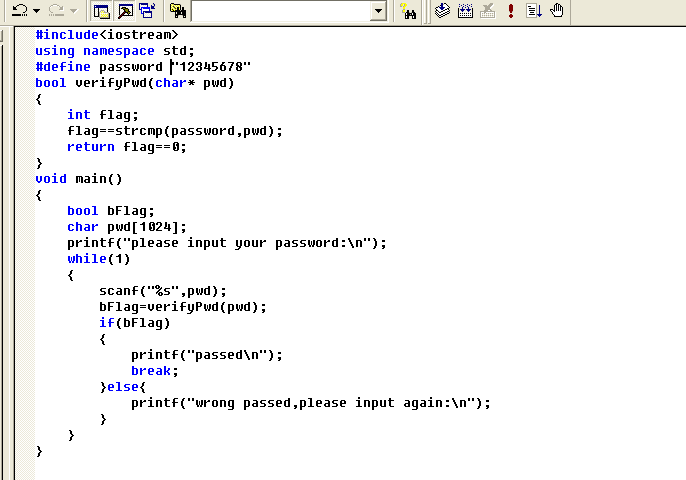
OLLYDBG软件破解

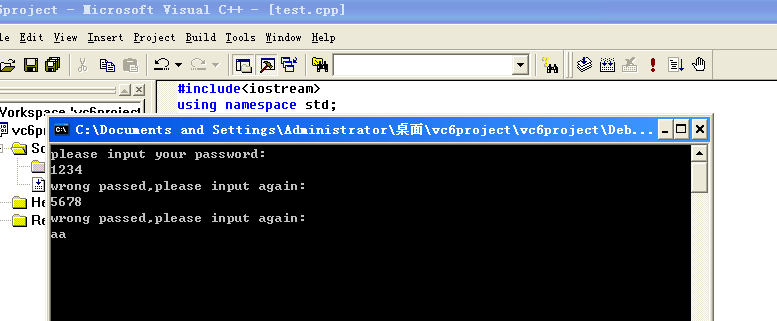
**实验要求：**

1.请在XPVC6生成课本第三章软件破解的案例。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。

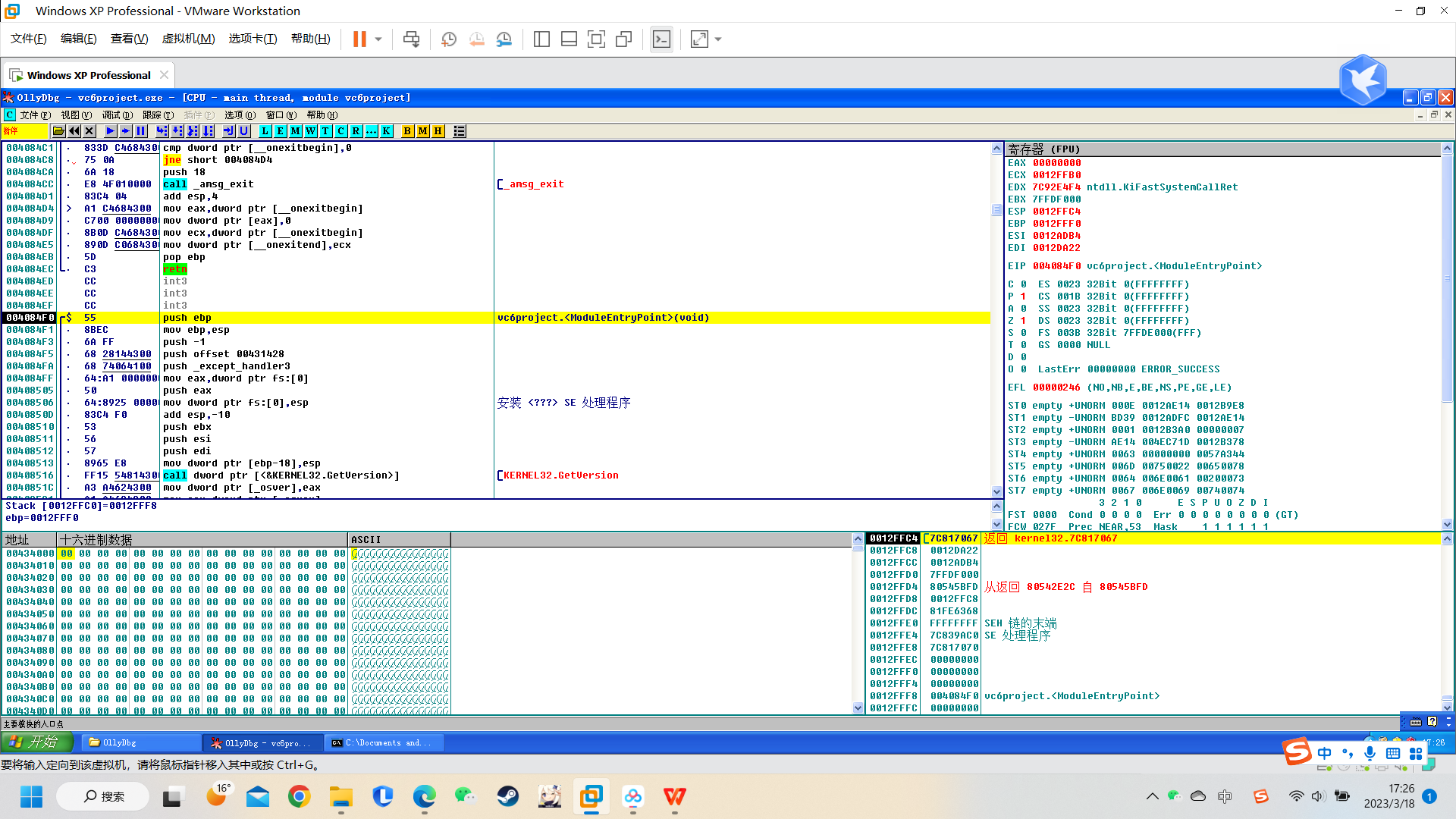
2.对生成的DEBUG程序进行破解，复现课本上提供的两种破解方法。

**实验过程：**





1. 写入代码，debug模式，形成.exe文件



用OllyDbg打开文件，可见汇编代码

对verifyPWD函数中flag==0的汇编代码进行解释：

Call strcmp ;调用比较字符串函数

Add esp,8 ;回复栈

Mov dword ptr [ebp-4],eax; 将函数返回值赋给变量[ebp-4]即flag

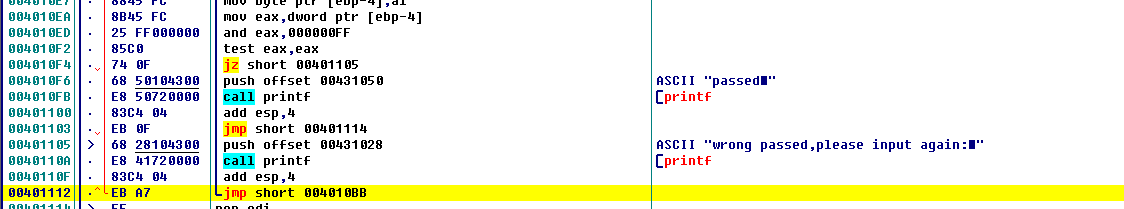
Xor eax,eax ;eax清零

Cmp dword ptr [ebp-4],0;比较flag与0

Sete al ;根据上一条指令的比较结果赋值al

2.破解方法一：（**输入错误口令时）更改跳转**

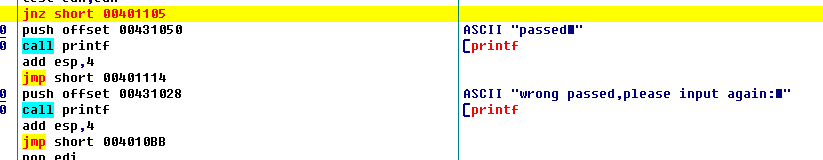
右键-查找-查找所有引用的字符串（或者ctrl+F）



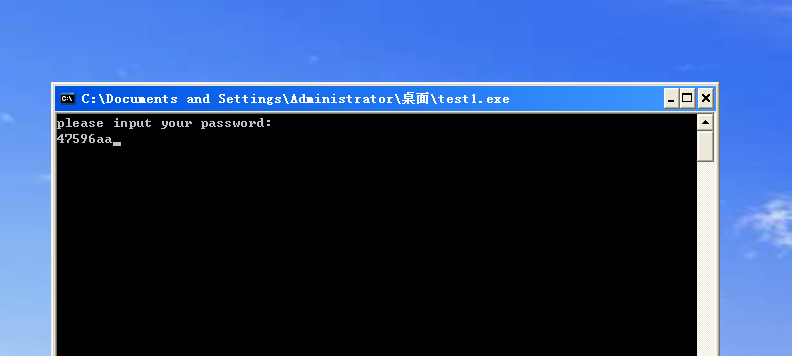
可知，满足判断条件为0时，跳转到“wrong”输出语句

此时破坏跳转逻辑：不为0跳转。

操作为双击jz，修改为jnz，空间大小不变。



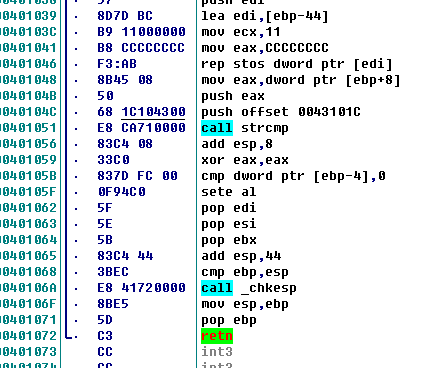
此时，错误答案将进入原本正确答案的跳转



若输入正确答案反而显示wrong

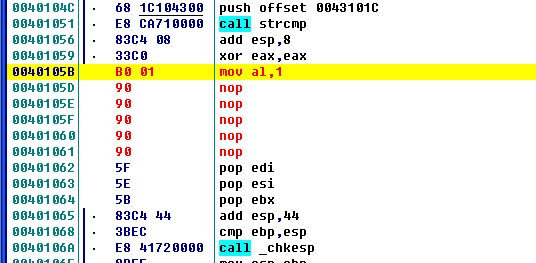
3.破解方法二：**强制控制返回值，劫持控制流，转入正确逻辑**

跟随调用函数



Ret返回前，有al的设置

此时我们通过更改cmp语句强制更改al的值

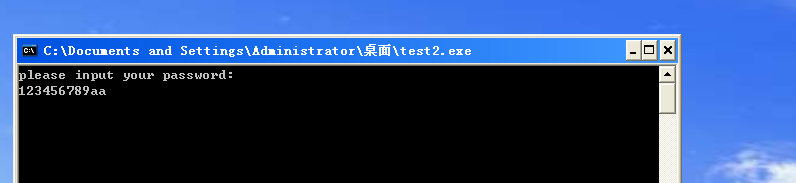


Cmp语句改为mov al,01

Sete语句改为nop

此时无论任何条件，al总为1

保存可执行文件，可以发现，此时无论输入答案正确与否，都会转到核心业务逻辑



至此，两种破解复现完成

**心得体会：**

加深了对汇编语言中的跳转、分支指令的理解；

明白了一些软件调试的基础方法；

学习并运用了调试分析工具（OllyDBG）;

进一步了解软件安全、软件破解