《漏洞利用及渗透测试基础》实验报告

姓名：姜志凯 学号：2011937 班级：信安班

**实验名称：**

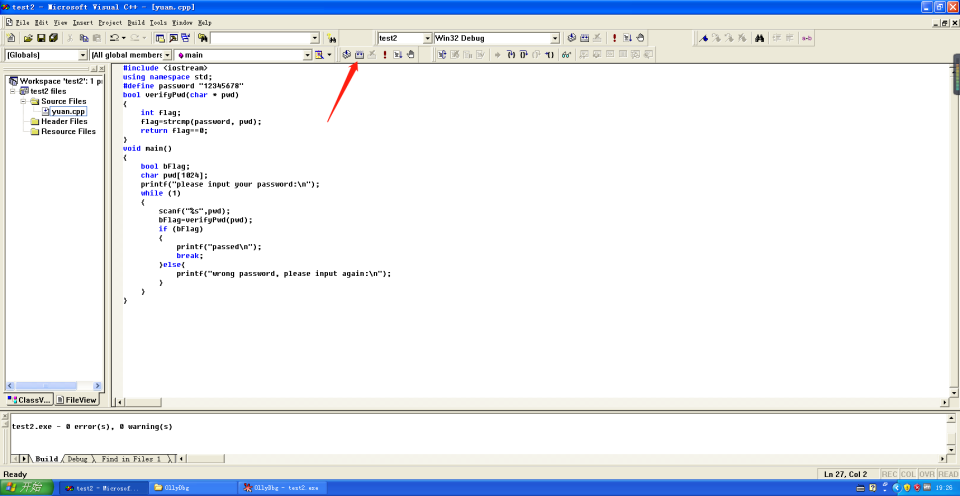
Ollydbg软件破解

**实验要求：**

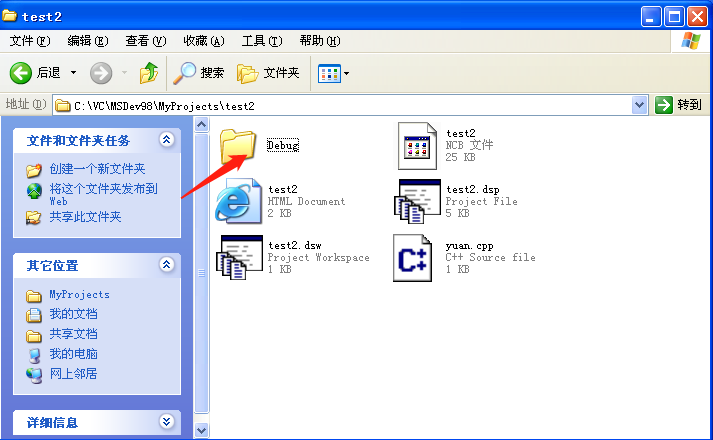
1. 在XP VC6生成课本第三章软件破解的案例（DEBUG模式，示例3-1）。进而，使用ollydbg进行单步调试，获取verifyPWD函数对应flag==0的汇编代码，并对这些汇编代码进行解释。
2. 对生成的DEBUG程序进行破解，复现课本上的两种方法。

**实验过程：**

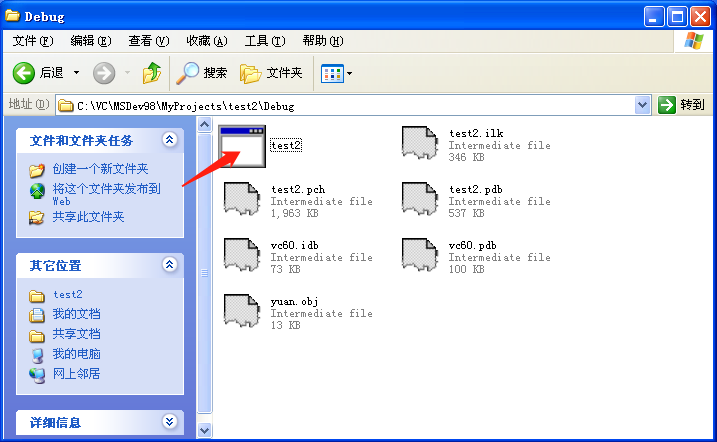
1.在xp vc6生成破解案例debug模式：

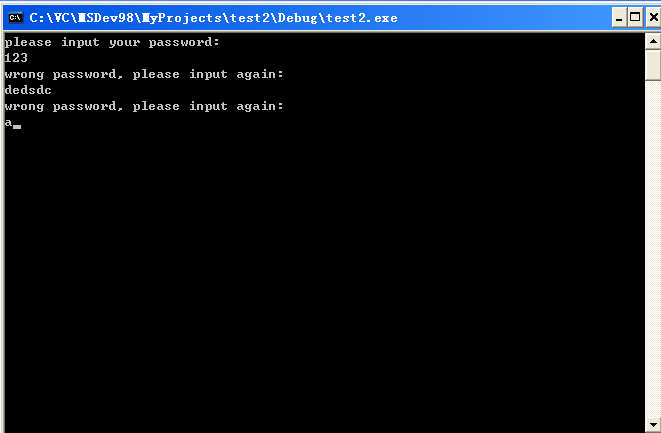


然后到目录中找到Debug文件



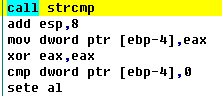
打开里面的test2.exe文件





只有输入12345678才会通过，进入主进程，其他password都会提示重新输入

使用ollydbug打开进行单步调试，获取得到verifyPWD函数对应flag==0的汇编代码如下：



call strcmp调用strcmp函数，比较两个字符串，相等则返回0，存在eax中；

mov dword ptr [ebp-4],eax 将函数返回值赋值给变量flag

xor eax,eax 清空eax的值

cmp dword ptr [ebp-4],0

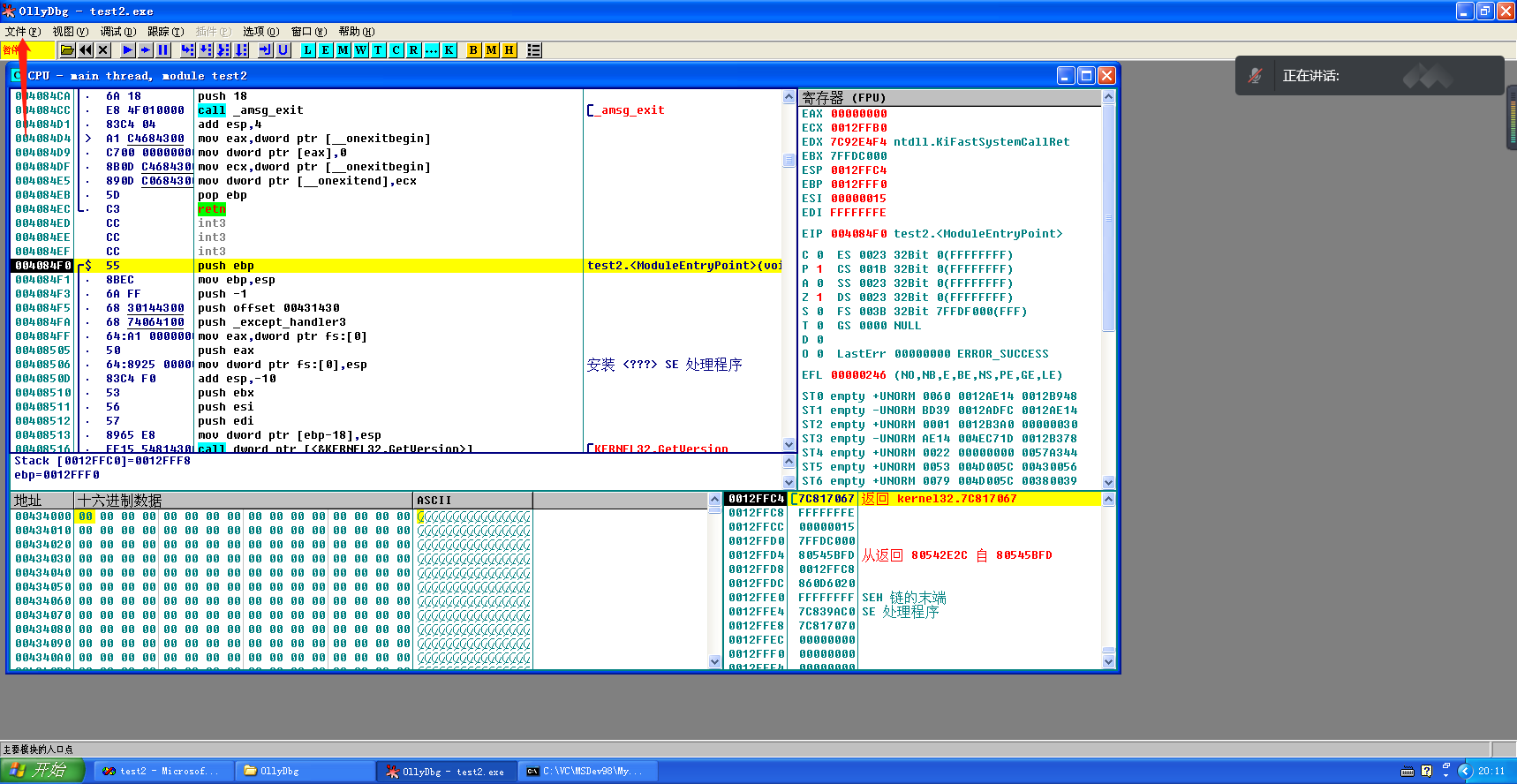
seta al 比较flag和0的值，如果相等则将al寄存器置为1，反之置为0

函数的返回值为eax寄存器的值，即若密码正确，函数返回1，否则返回0

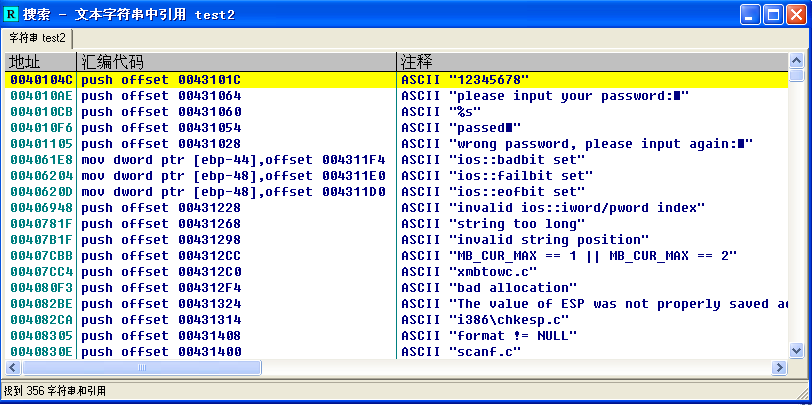
2.两种破解方法：

（1）修改语句Jz short 0041364b为Jnz short 0041364b，当输入密码不正确时，通过；正确时，重新输入

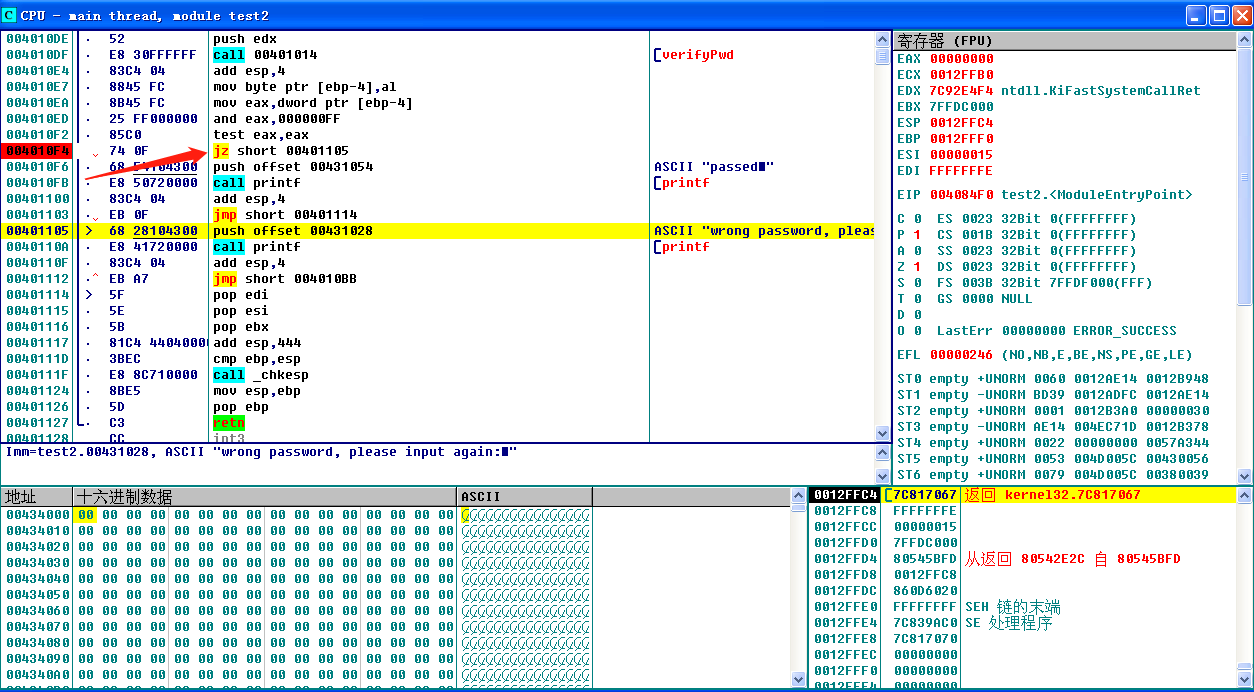
选择文件打开test2.exe



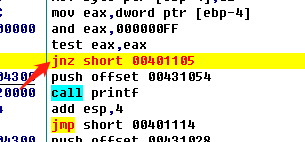
右键选择查找-所有字符串引用

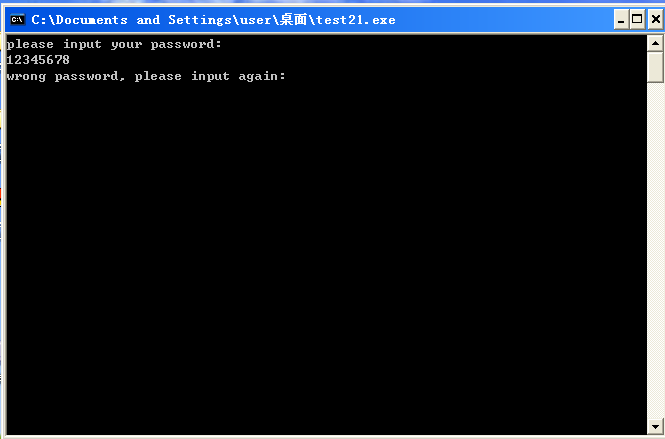


Ctrl+f输入“wrong”，定位到错误时的输出的位置



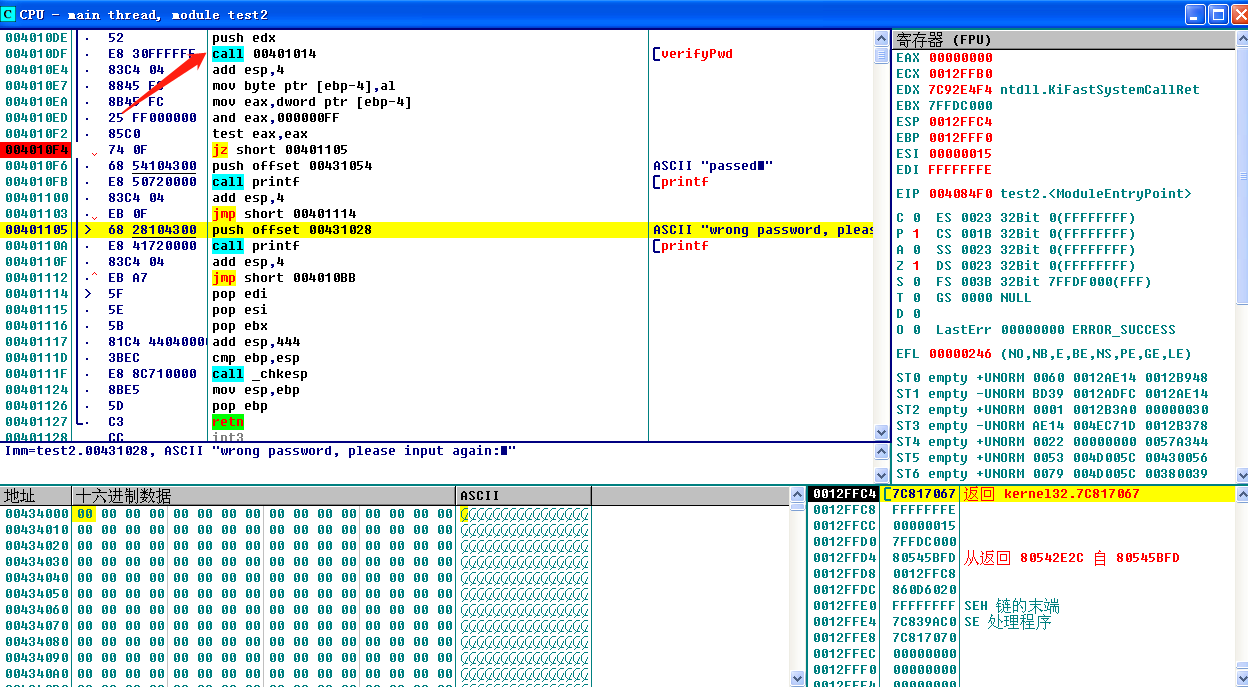
注意到前边有一个Jz short 0041364b，将其改为不一致时跳转Jnz short 0041364b



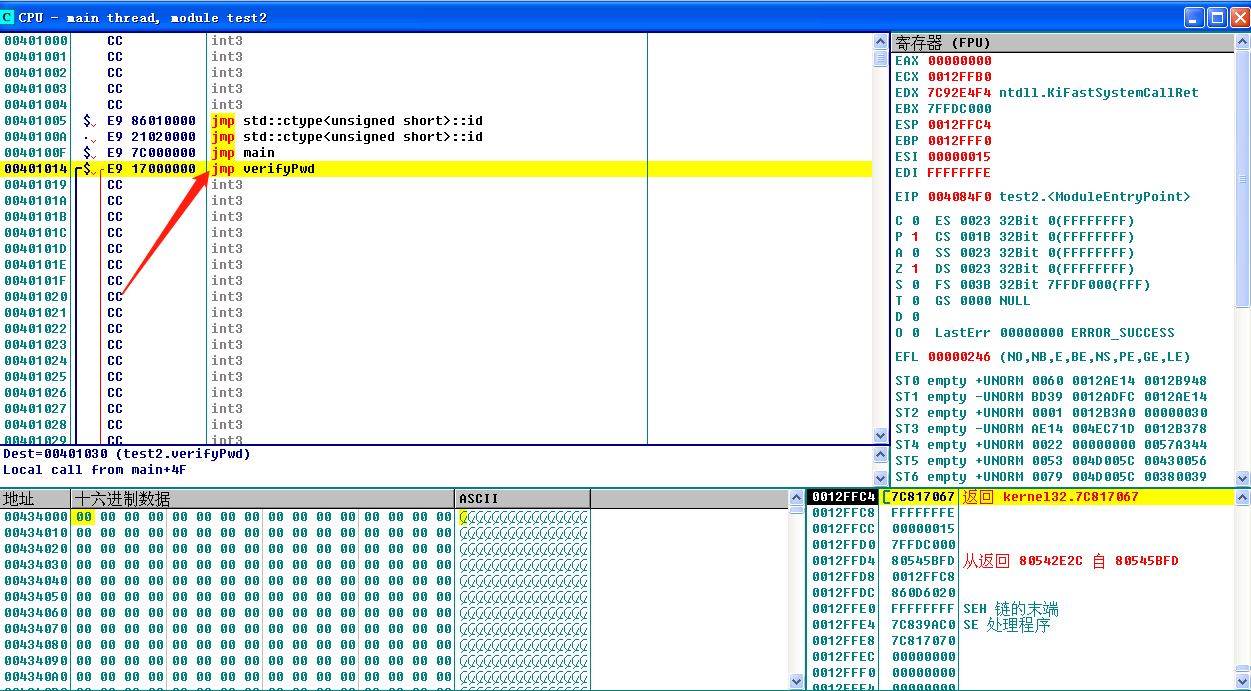


此时输入正确的密码不能通过，随便输一个就过。

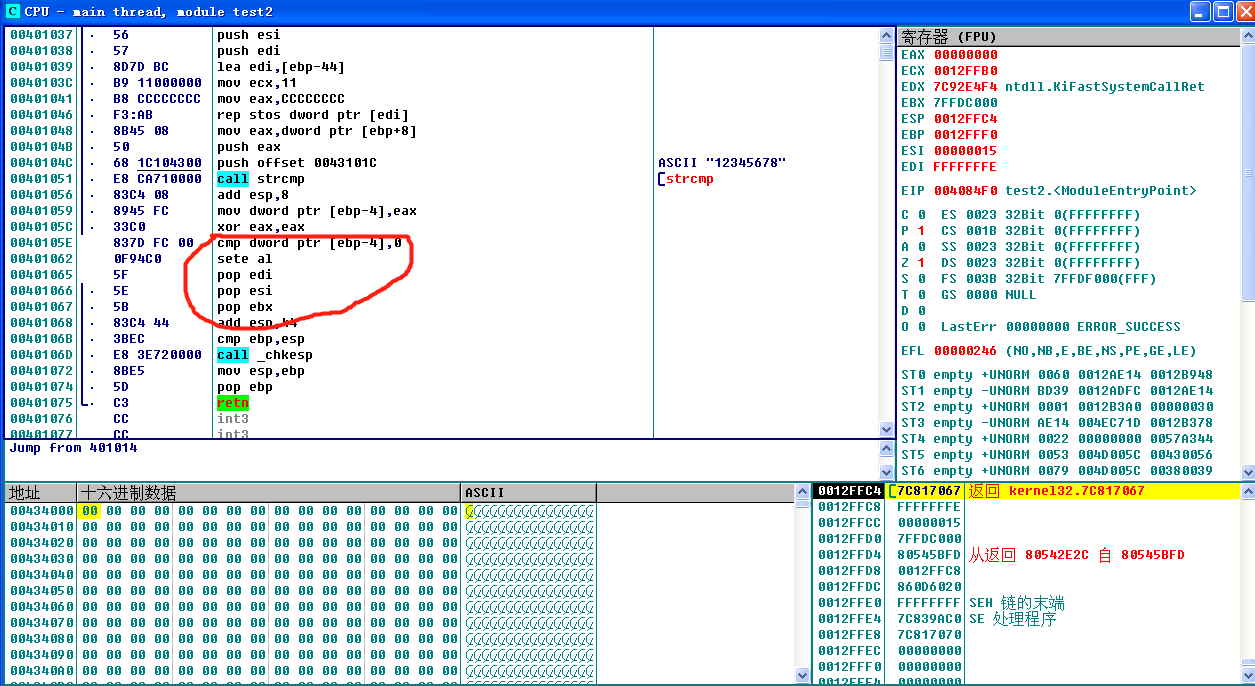
（2）将verifyPwd函数返回值设置为恒为1



前边有一个调用函数，右键跟随



继续右键跟随



这里是比较flag和0，若相等则将al置为1，反之置为0，eax即为返回值

所以这里直接将al赋值为1即可，这样，无论输入什么，函数返回值均为1，均能通过。

修改如下：

