《软件安全》实验报告

姓名：曹瑜 学号：2212794 班级：密码科学与技术

**实验名称：**

OLLYDBG软件破解

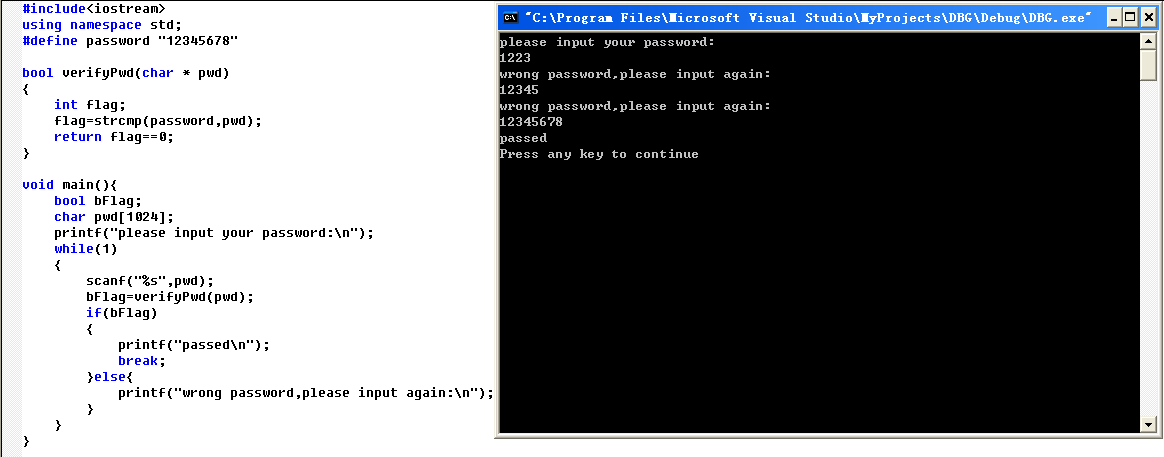
**实验要求：**

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。

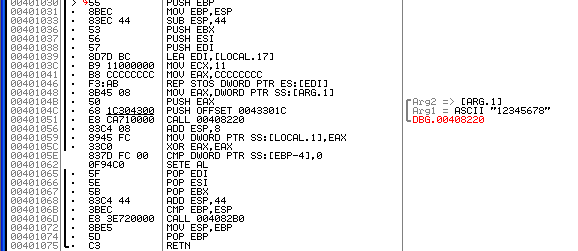
2. 对生成的DEBUG程序进行破解，复现课本上提供的两种破解方法。

**实验过程：**

1. 进入VC生成案例：



获取对应汇编代码：



 //将strcmp函数调用后的返回值存赋值给变量flag

 //清空eax的值

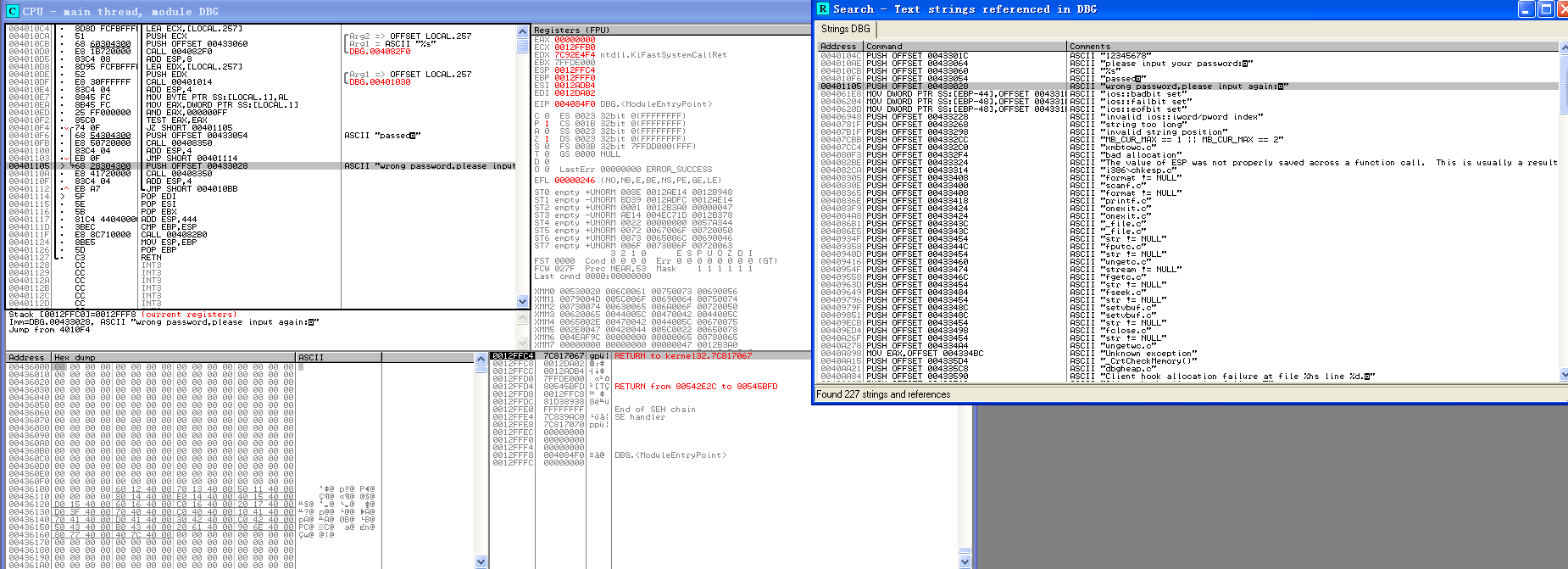
 //比较flag与0的值，即flag==0

 //根据状态寄存器的值，相等则设置，不等则不设置

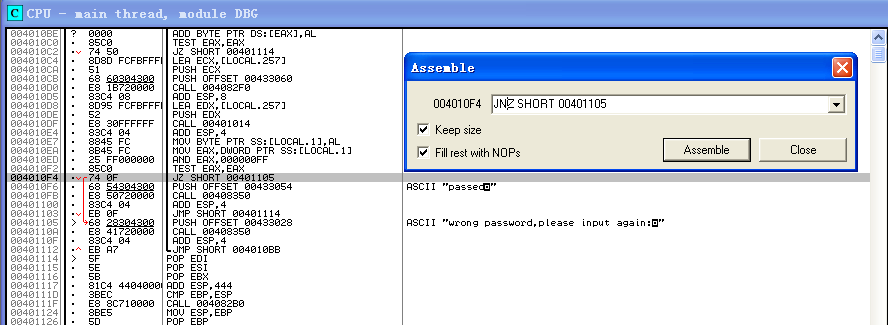
1. 使用ollyDBG进行破解：

**A.方法一**

1.1 查找引用字符串，查找“wrong”语句



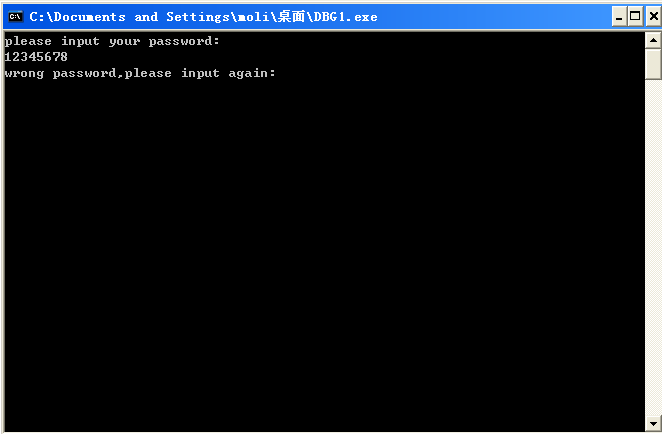
1.2 定位到输出错误判定的语句，修改跳转判断语句逻辑，将JZ取反为JNZ



逻辑取反后的应用程序：

原密码12345678显示为错误密码，而随意输入的其他数字都显示为正确密码

破解成功



1. **方法二**

2.1将逻辑修改复原，可看到在跳转错误输出之前执行了call语句，跳转到对应函数中

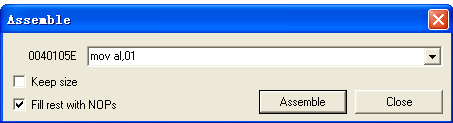


2.2在对应函数中修改逻辑，针对CMP和SETE

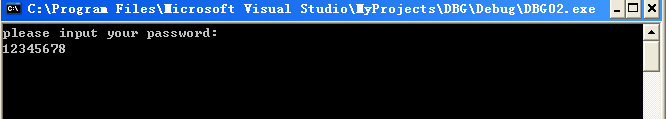
只有输入结果和真实密码比较值相等时才设置AL为0或1



现在强制性将AL置为01，将SETE AL 改为空指令



现在任何输入情况下AL都为1，此时每种输入都为正确输入,破解成功



**心得体会：**

通过实验，掌握了利用OLLYDBG对代码进行单步调试的方法，能获取函数对应汇编代码并进行理解，还复现了课本上两种破解程序的方法并成功破解，但调试过程中仍不熟练，希望今后的实验中能取得改进。