**《软件安全》实验报告**

姓名：禹相祐 学号：2312900 班级： 计科

**实验名称：**

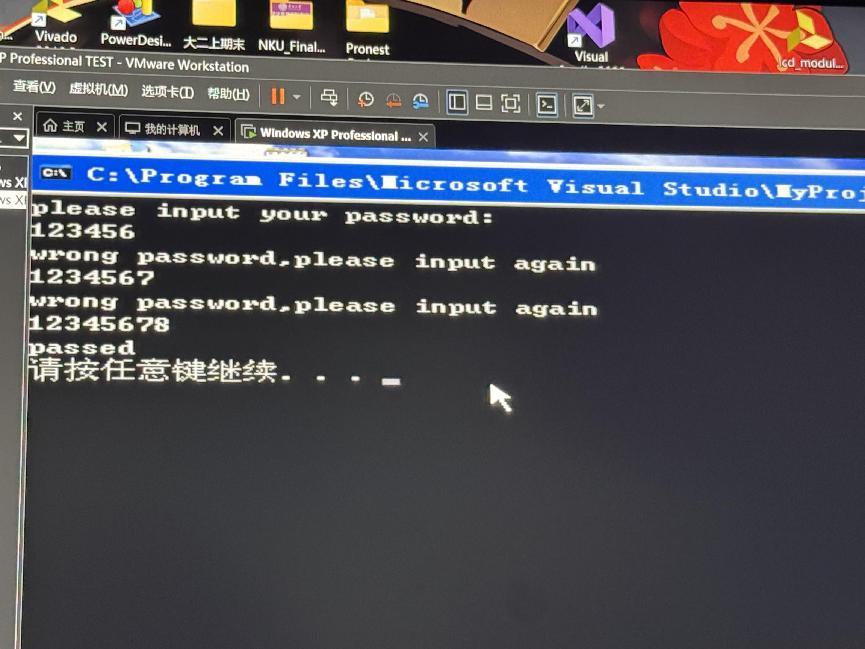
OLLYDBG软件破解

**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。

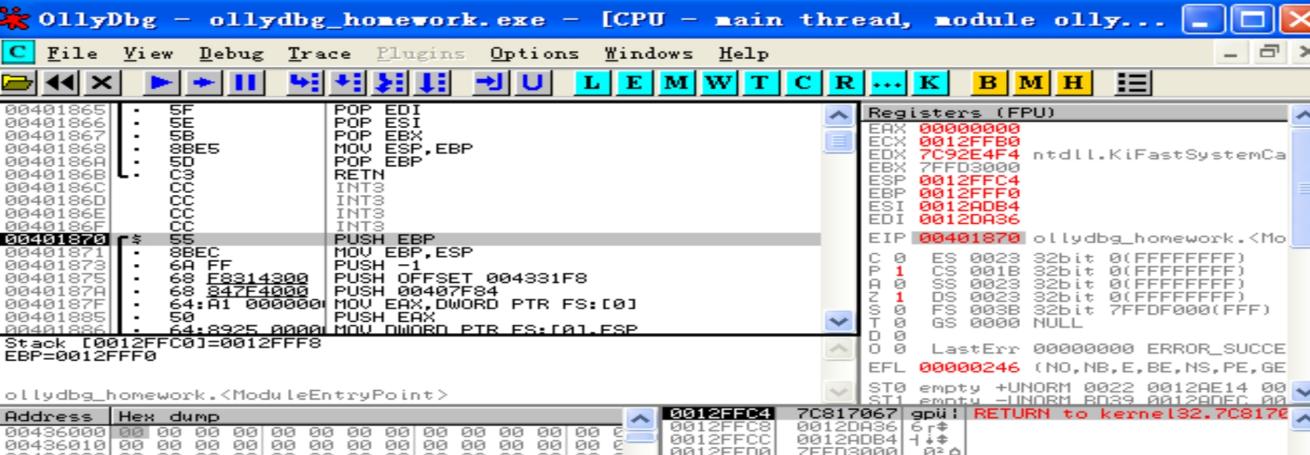
**实验过程：**

1. **OllyDBG的准备工作：**
2. 先在VC6下生成实验所用的exe文件,如图：

****

可以从此处看出：当输入的密码错误时，会再一次执行输入密码，并弹出“wrong password,please input again”并且再一次输入密码。直到输入正确密码“12345678”时，才会弹出“passed”。

1. 然后我们将此程序生成的ollydbg\_homework.exe拖入ollydbg进行测试，如图：

****

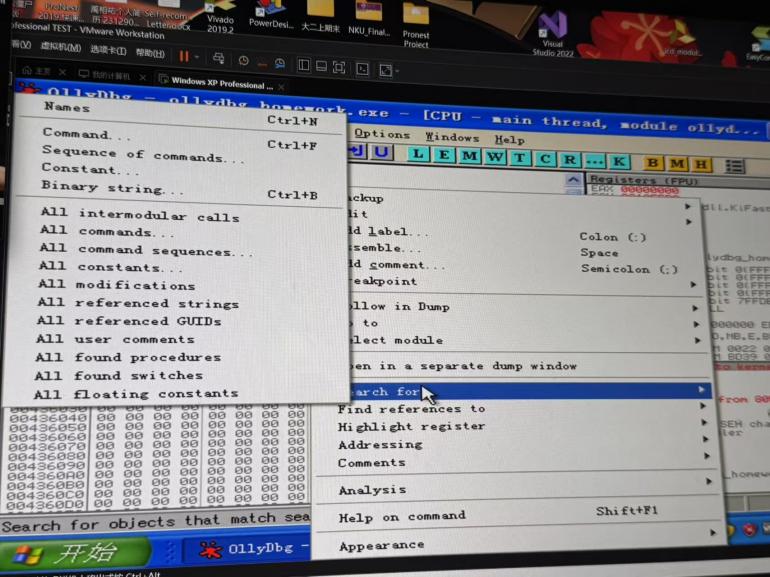
至此，已经完成所有准备工作，现在开始采用两种不同方式进行破解。

1. **两种破解方式：**

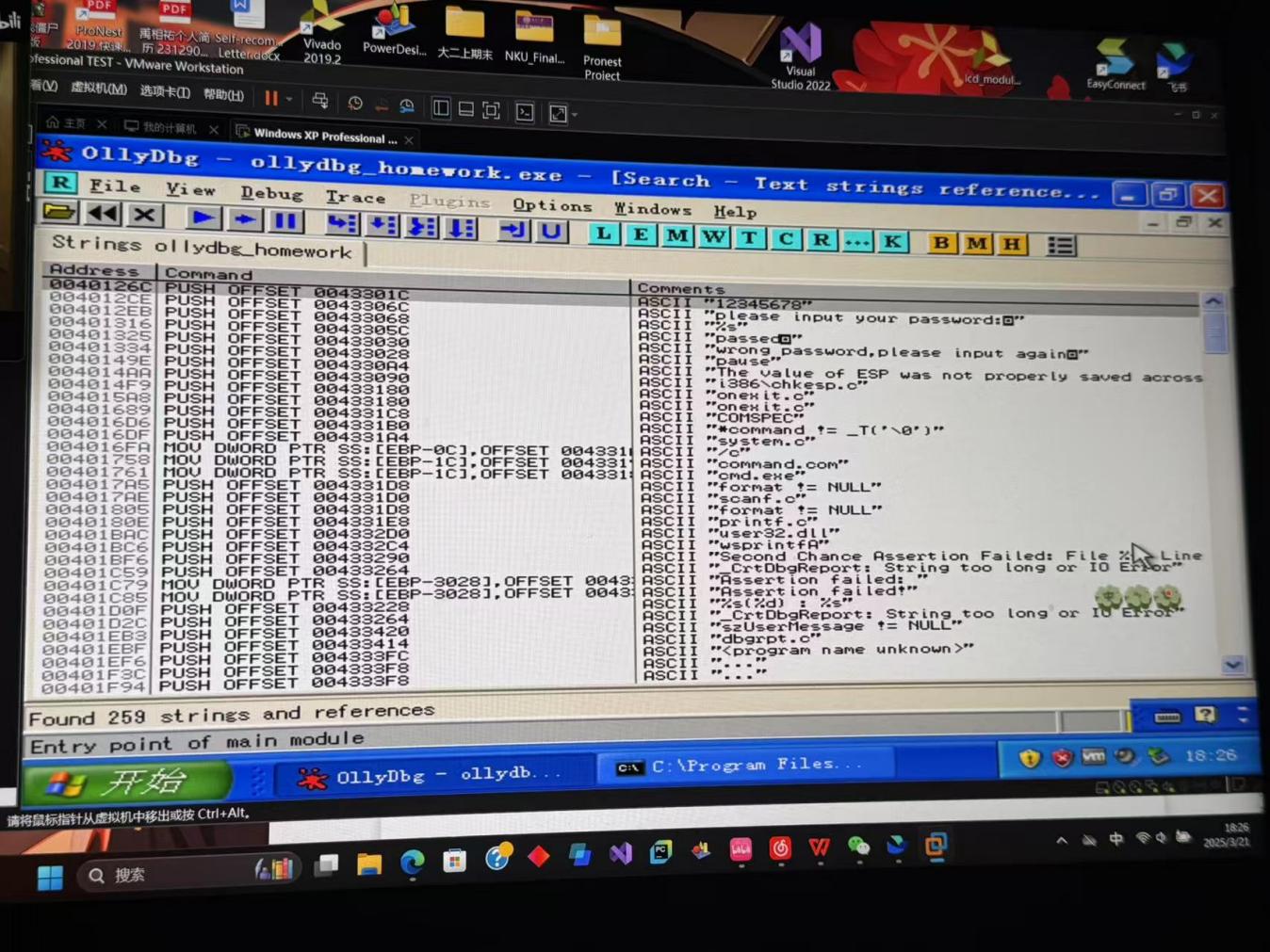
当我们想要破解时。我们首先要查看一下verifyPwd函数的汇编代码：

首先我们知道，在判断密码是否正确的时候，会有输出“passed”或“wrong password”的提示，那么我们可以根据输出的“wrong password”大致定位程序：

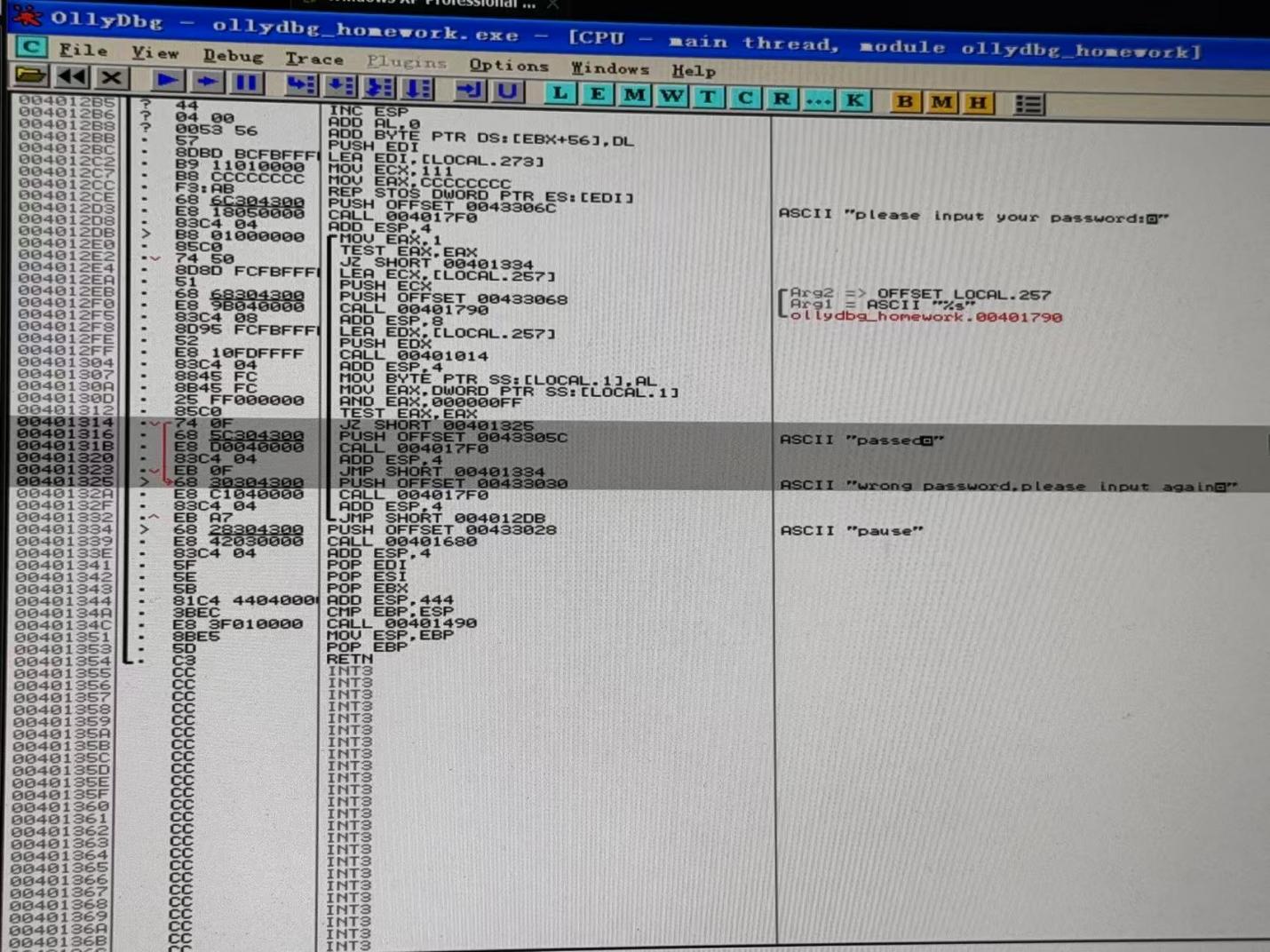
I)先右键选择“search for”再选择”all referenced strings”:



II) 我们可以看到“wrong password”（若看不到,可以ctrl+f直接查询“wrong”）



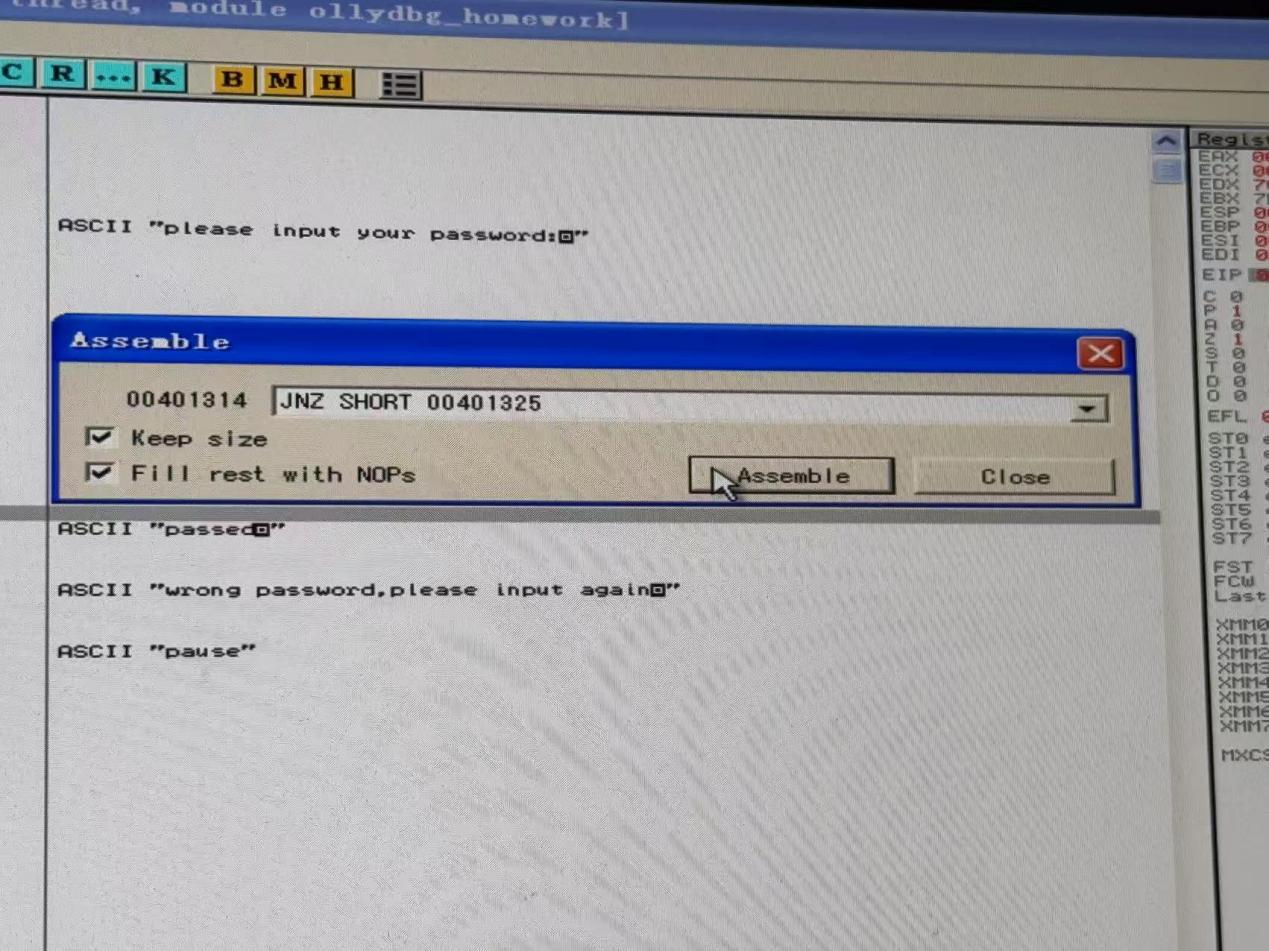
III)然后我们双击“wrong password”那一行就可以看到：



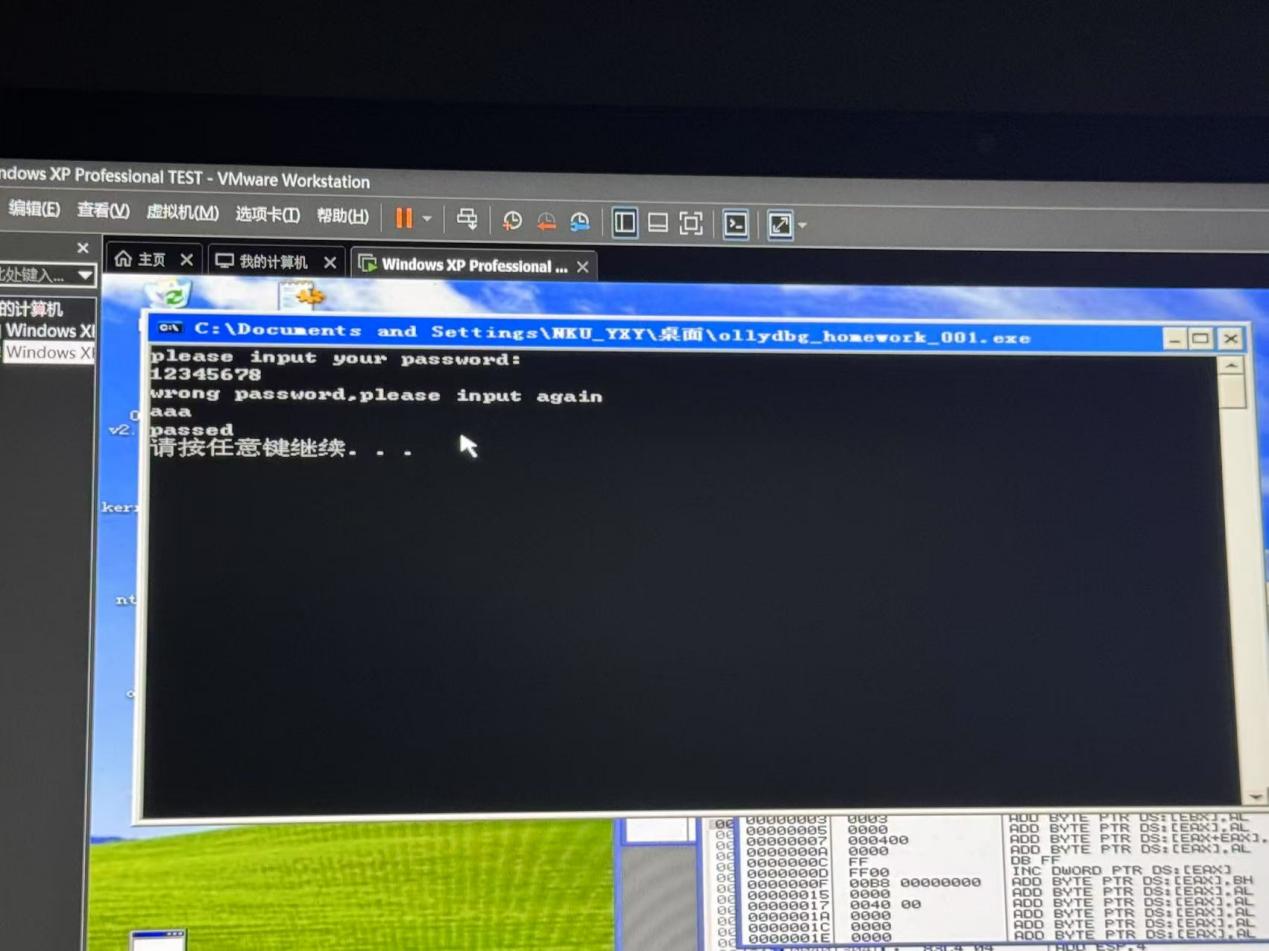
此处OllyDBG替我们标识了从何处跳转到了输出“wrong password”，也就意味着最上方的“JZ SHORT 00401326”承担了判断条件的作用。

因此，我们有了第一种的破解方法：就是让判断条件取反，即输入错误的时候才通过，输入正确反而显示“wrong password”：

这个实现也很简单，就是将此处的“JZ SHORT 00401326”改为“JNZ SHORT 00401326”,这个N指的是“not”，这样就轻松实现了条件的取反：



然后将文件保存为“ollydbg\_homework\_001.exe”，再试一次：

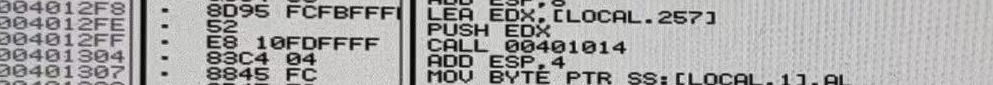


此处就能看出，输入正确答案“12345678”输出了“wrong password”，输入错误答案“aaa”反而输出了“passed”,第一种方法实现。

接下来是第二种方法：

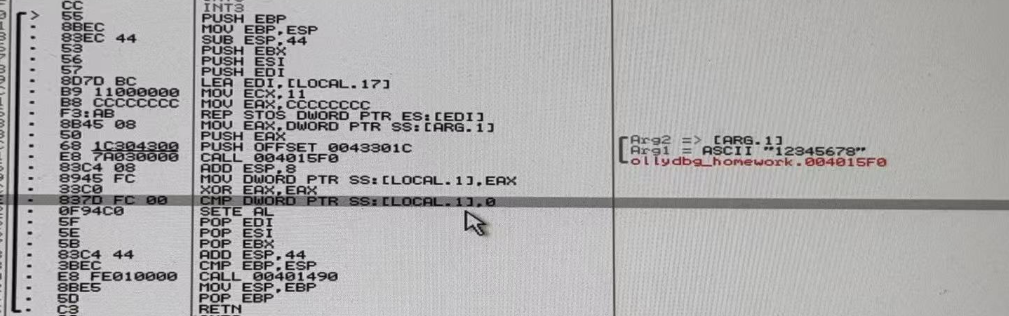
既然存在verify\_pwd函数，那我们也可以试着让这个函数始终返回true，这样无论输入什么都会显示“passed”。

I)那我们先实现对于verify\_pwd函数的定位：



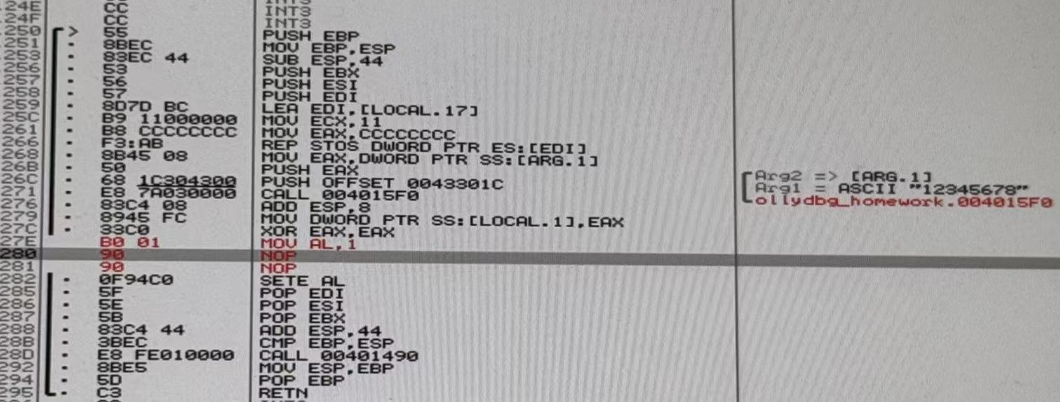
即此处的“call 00401014”

II)然后右键并连着两次“follow”，就会到如下页面：

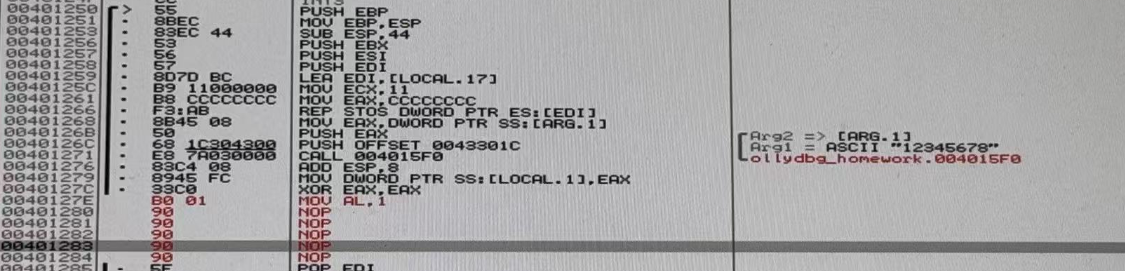


可以从代码得知，当返回的时候会有个比较产生的bool值，可以定位到SETE AL

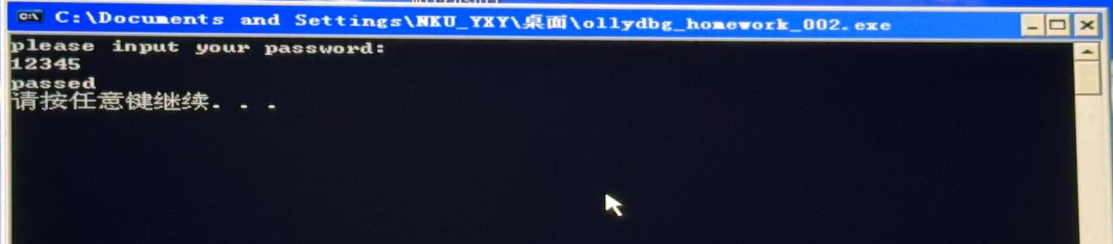
，接着考虑相关的“CMP DWORD PTR SS:[LOCAL.1].0”。易知此处是产生bool值的指令，考虑将其始终设置为1，修改为“mov al,1”：



然后接着将“SETE AL”修改为空指令“NOP”:



然后保存为“ollydbg\_homework\_002.exe”，执行如下：



至此两种方法均得到实现。

**心得体会：**

通过这次实验，我学会了使用ollyDBG进行基本调试的方法，也掌握了几个基本操作，比如：通过“follow”操作实现程序的跟随，通过“searching string”查找对应字符串，实现定位，也学会了利用基本的汇编语句的更改实现简单程序的破解。

通过这次实验，我也更进一步熟悉了汇编语言中的寻找、判定，也对汇编语言的语法有了更深的了解，这次实验很有收获！