《漏洞利用及渗透测试基础》实验报告

姓名：艾明旭 学号：2111033 班级：1121

**实验名称：**

ollydbg软件破解实验

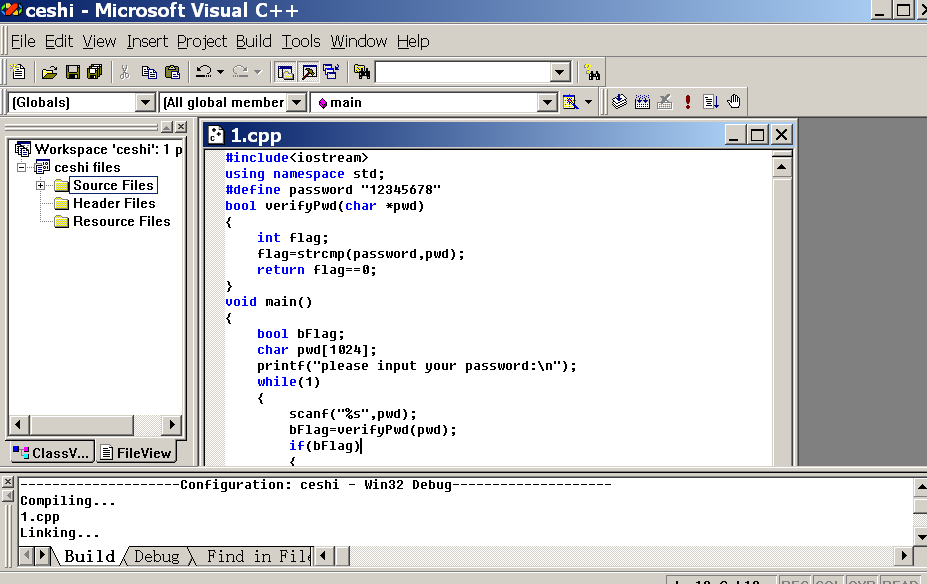
**实验要求：**

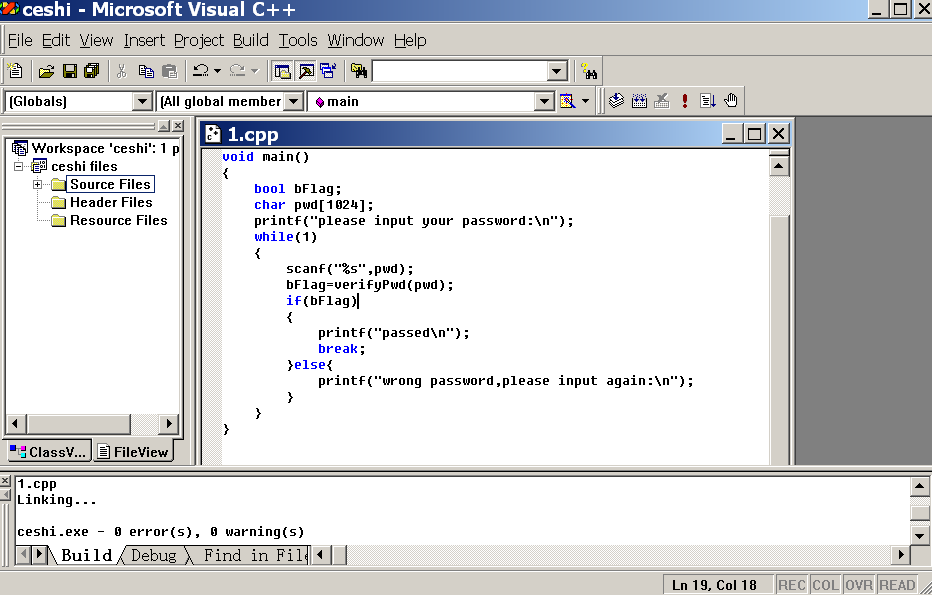
根据第三章示例，在XP环境下进行VC6反汇编调试，并且在ollydbg下打开并运行相关程序，通过进行渗透可以不输入密码就能直接得到最终结果。

**实验过程：**

1. 进入VC反汇编

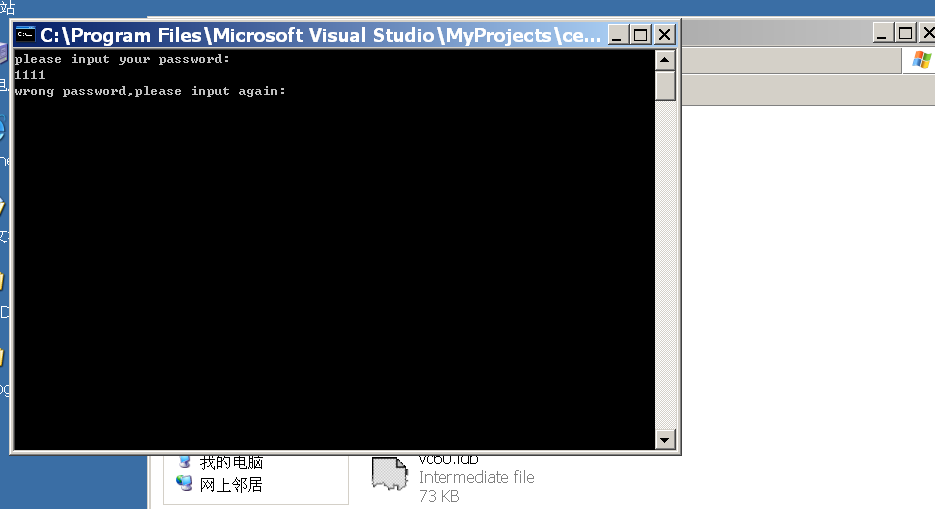
打开虚拟机的xp系统后，在vc6中创建win32的控制台文件，添加源文件后将代码复制到源文件中，debug无误后，得到相关的程序。



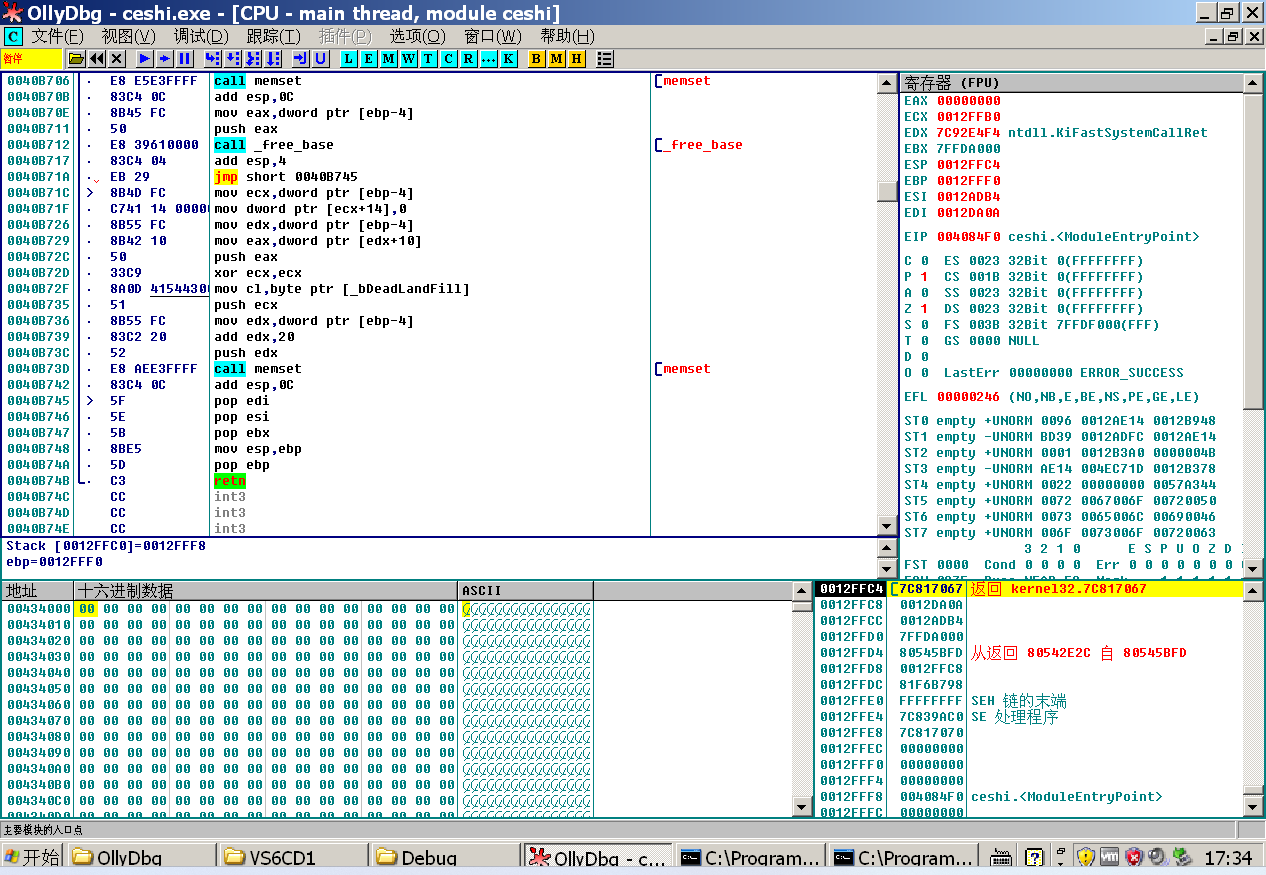


2. 打开相关程序

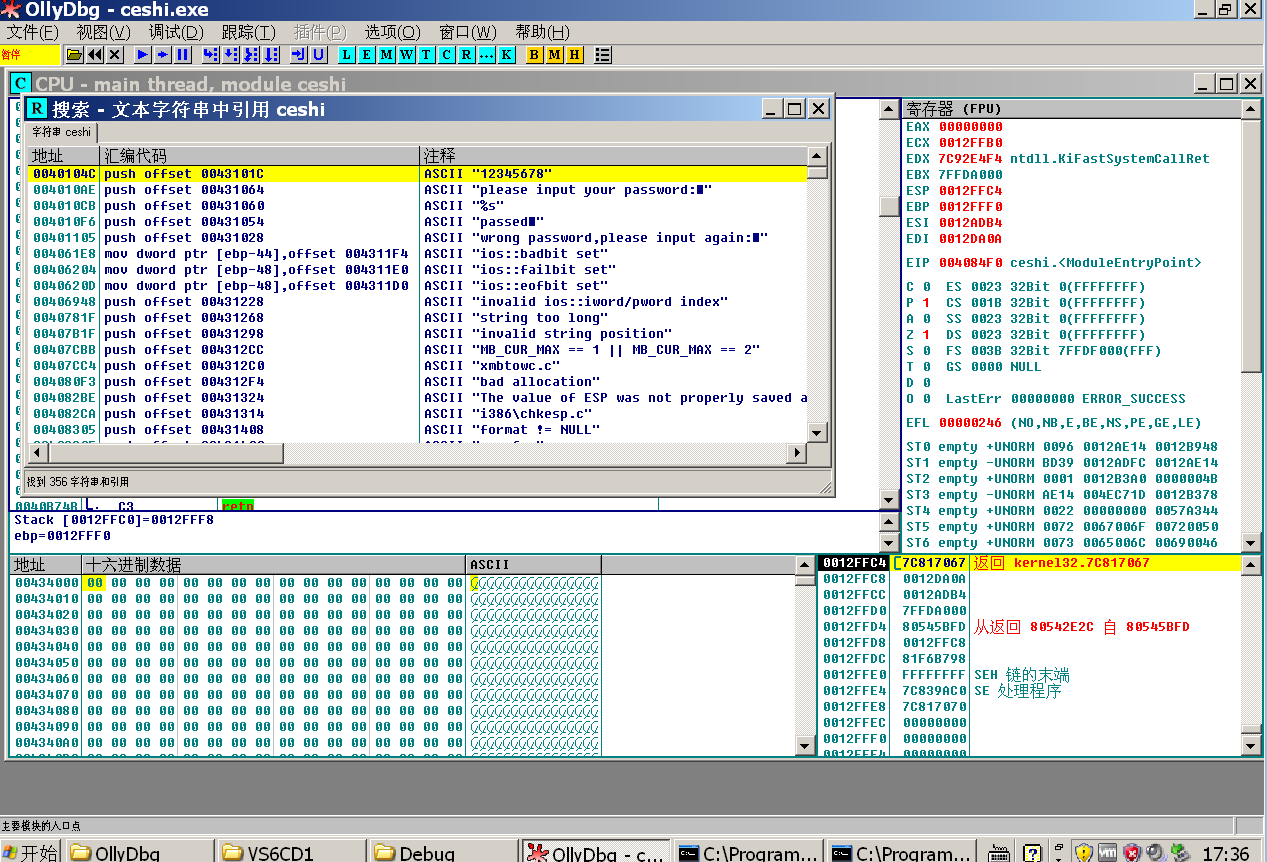
在文件夹里把相应的程序打开，发现可以打开相关的程序，其中我们如果不输入正确的密码，就无法得到最终的结果。



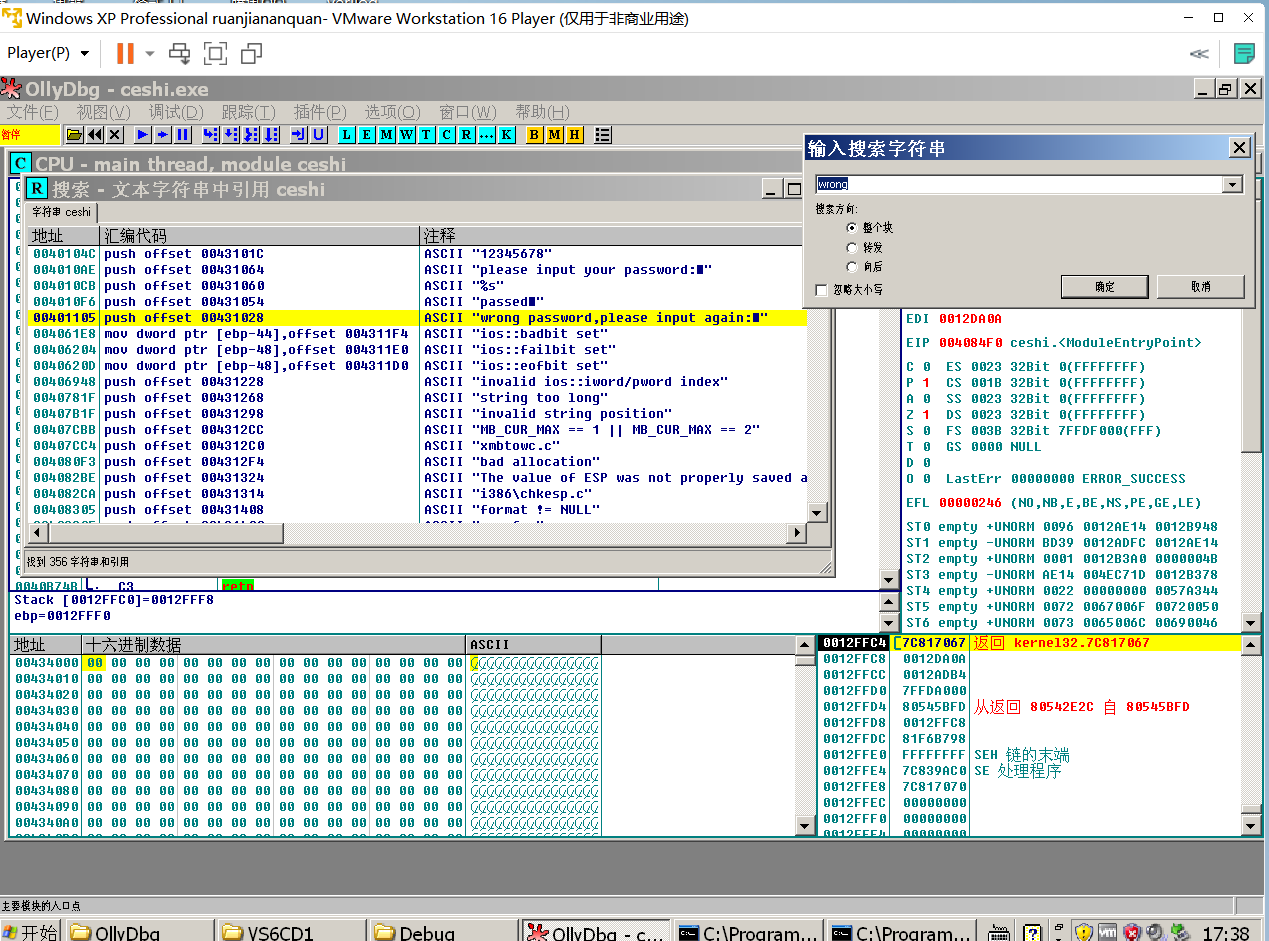
3. 在ollydbg当中打开相应的程序



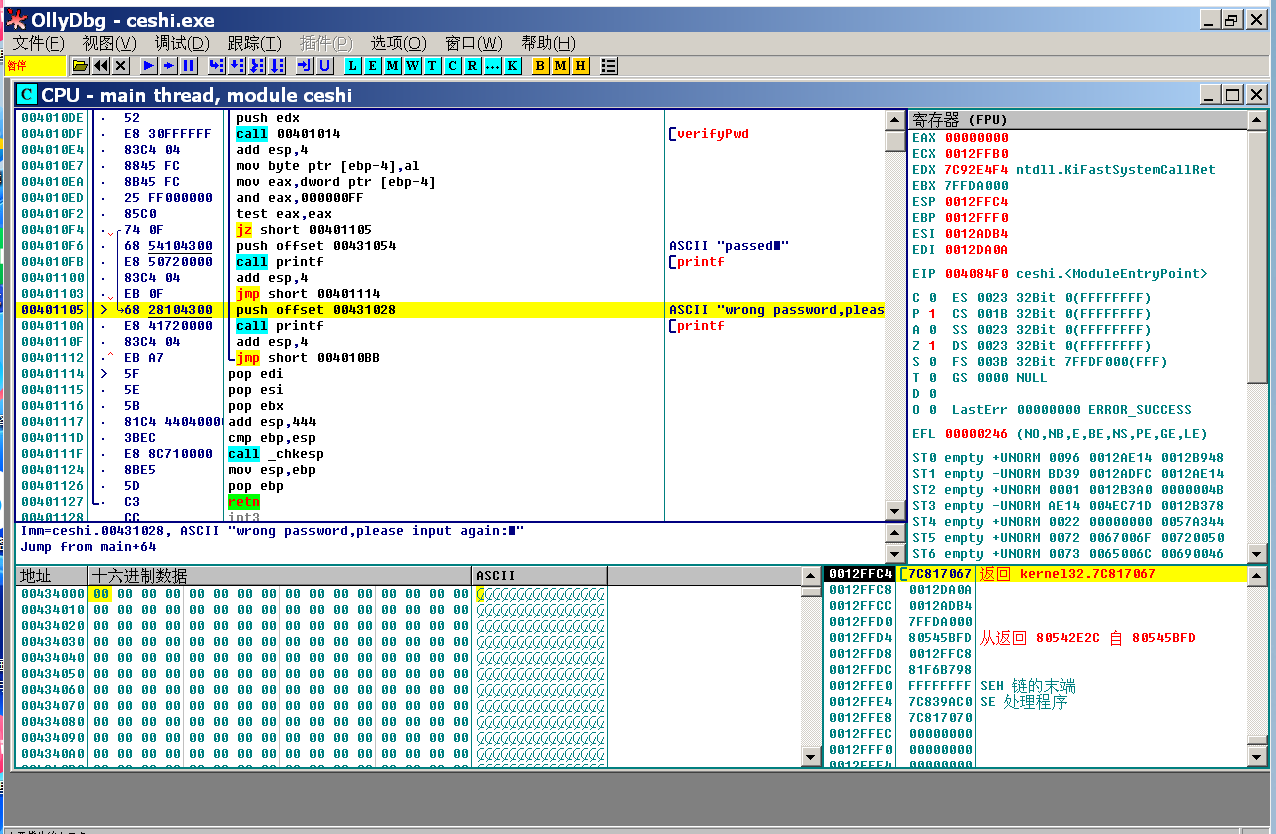
使用查找——查找所有引用的字符串得到所有的字符串所在的位置



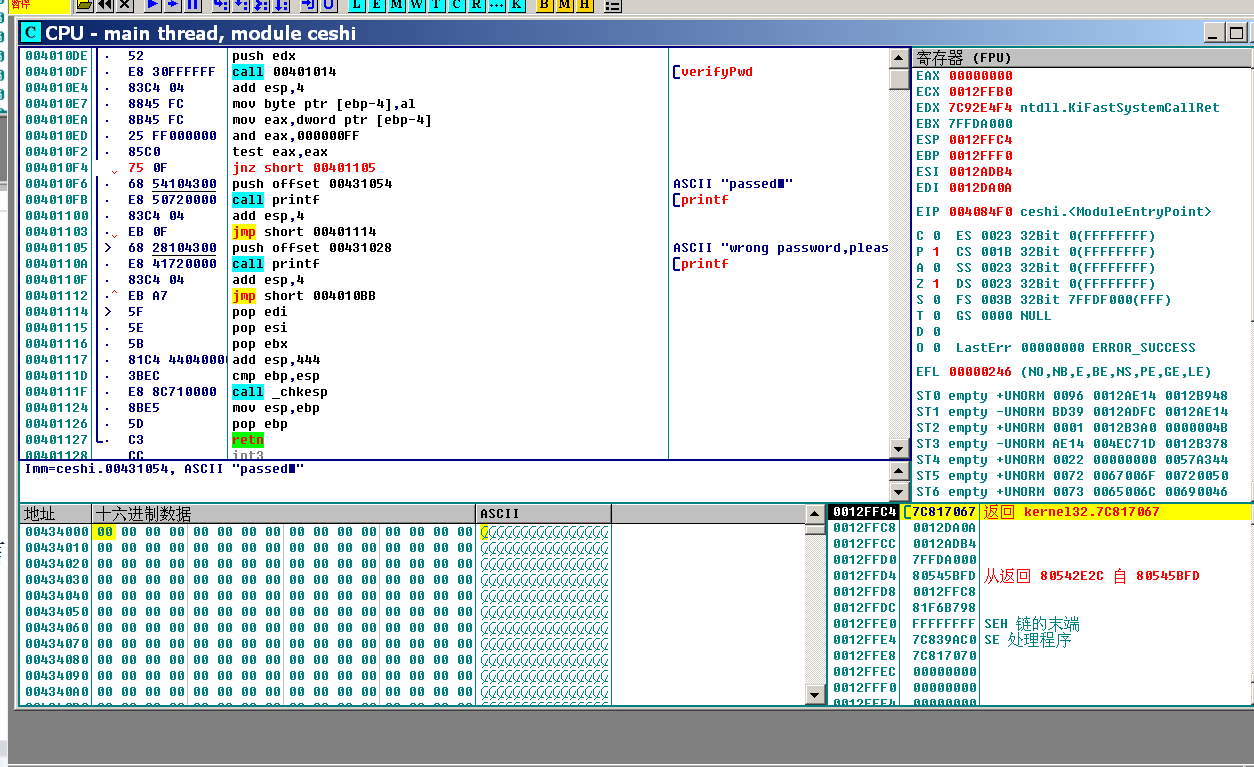
按下ctrl+f，使用查找工具找到有wrong字符串所在的地方。



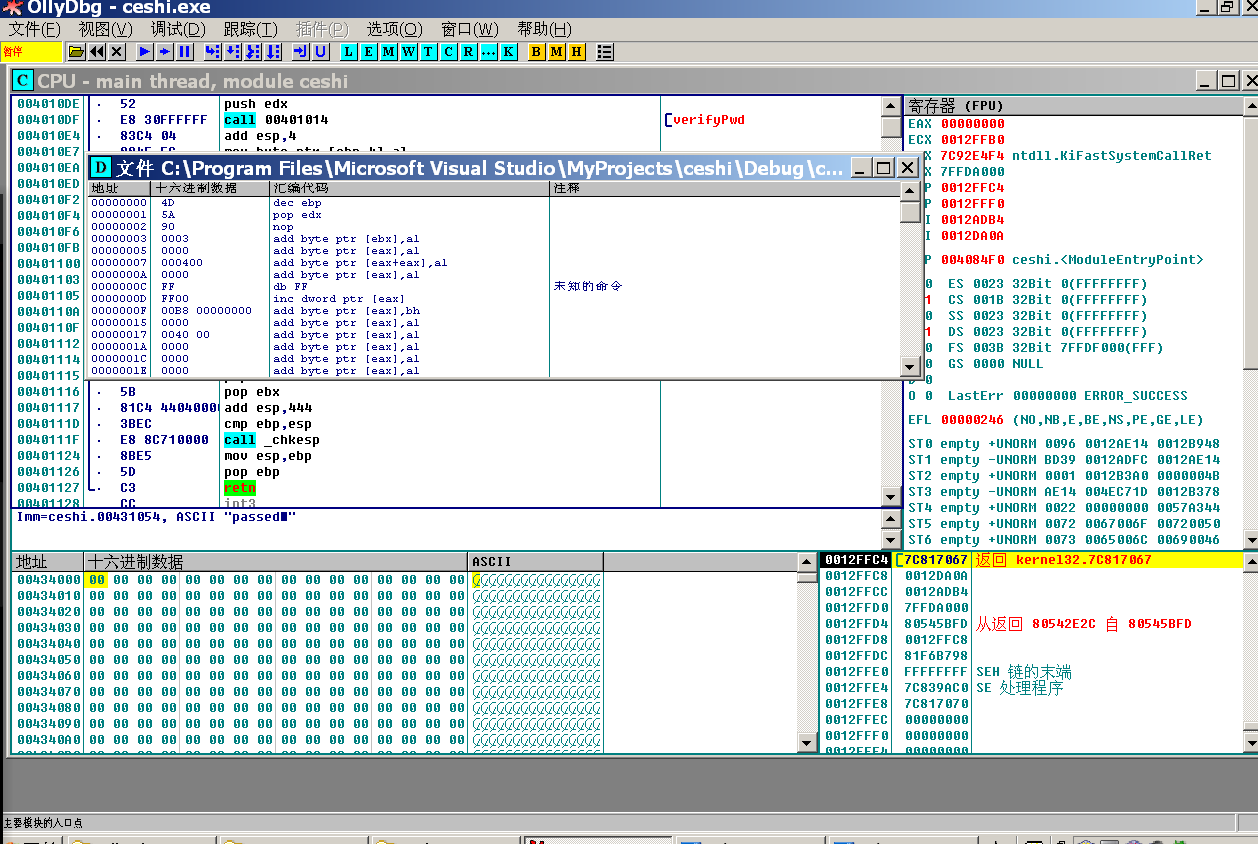
双击后可以看到相应的汇编代码语句。



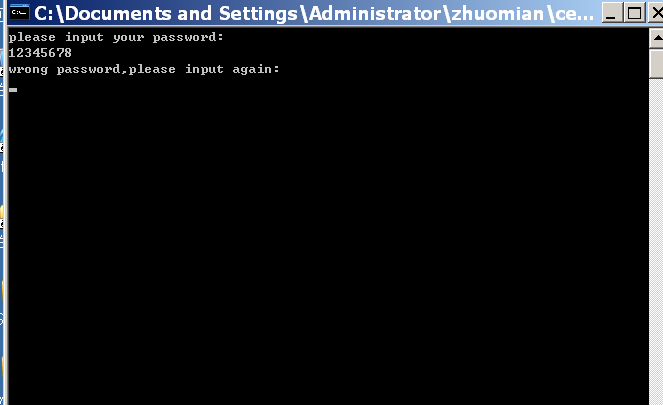
看到相应的反汇编代码之后可以双击



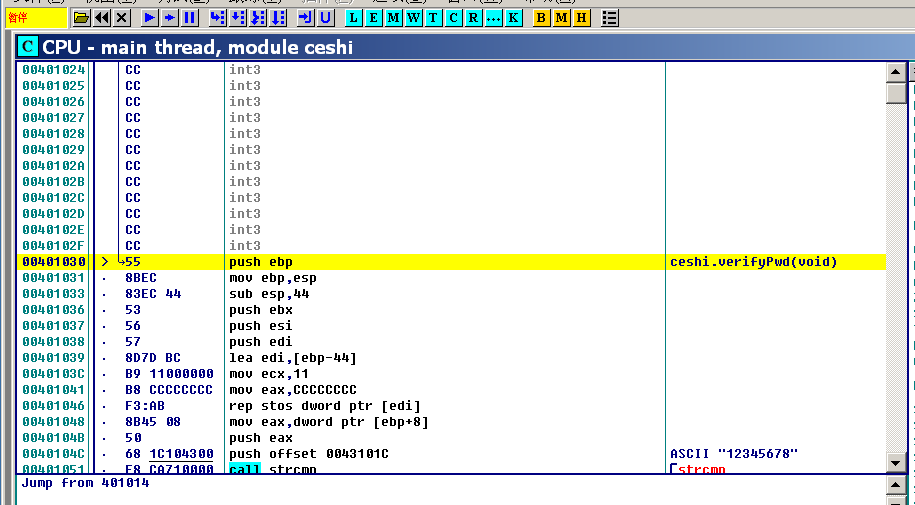
利用修改把jz逻辑语句修改为jnz语句，这样在逻辑上可以打到啊一种取反的目的，便可以得到与原实验结果相反的 实验结果，编辑之后复制所有修改到可执行文件，并且保存修改后的文件



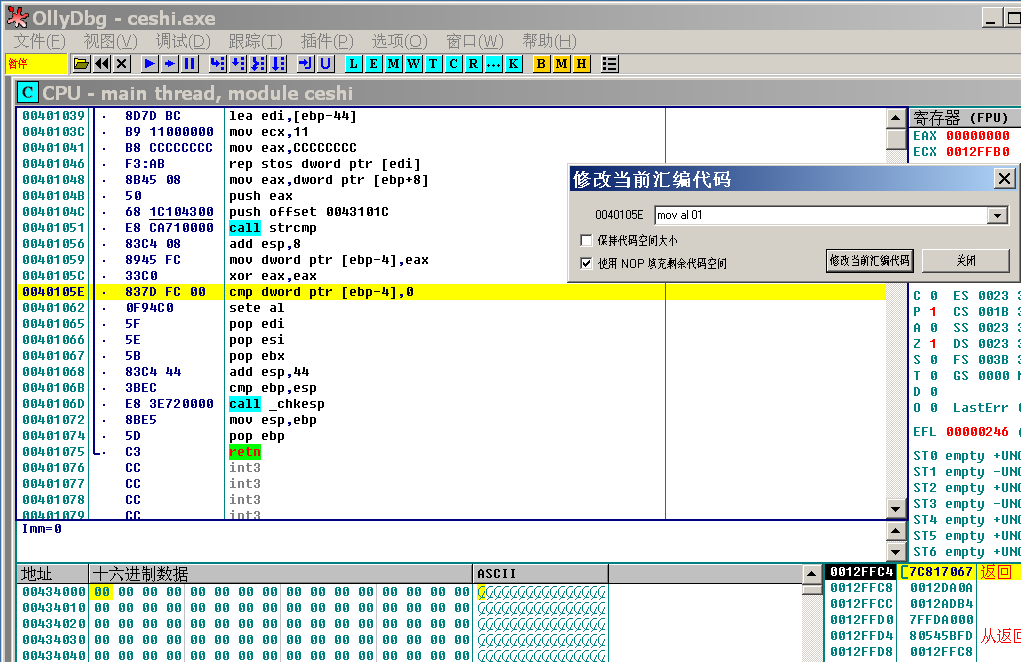
之后再打开相应的文件，就会发现我们输入正确的密码之后就会出现



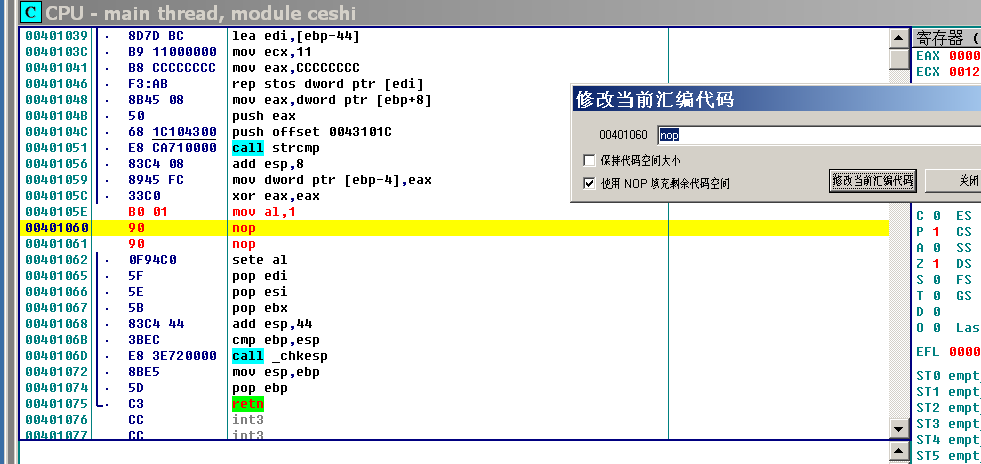
把反汇编代码调回修改之前的状态，同时我们观察到上面还有调用相关的函数，我们右键之后跟随，得到一个需要跳转的地方之后继续跟随，得到相应的函数位置和内容。



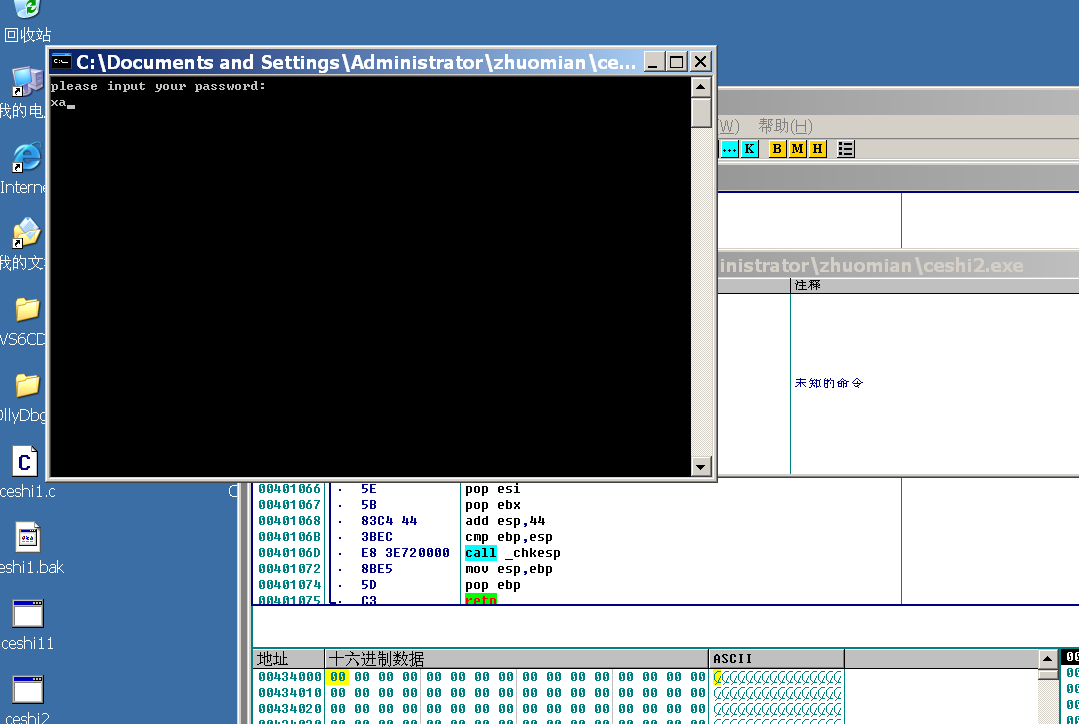
我们找到逻辑当中使用了一步cmp语句，进行比较之后才有决定是否跳转到最终的结果的相应语句。，所以我们使用mov语句对相应的逻辑进行更改，把它变成强制跳转到相应的地址，使用mov语句的同时，我们不选择保存代码空间的大小，把原本的cmp所占用的空间直接修改为一句话，使我们需要的时候就可以直接跳转到相应的地址而不经过任何的比较。



修改完之后我们看到下面的sete al指令仍然没有相应的结果，所以我们需要把它也修改为nop指令设置为空。



同上进行编辑复制所有代码到可执行文件，保存文件为可执行文件之后，就能得到一个程序，这个程序当中我们不论输入任何的密码，都能成功的跳转到相应的位置，结束相应的程序。



**心得体会：**

通过实验，我掌握了通过ollydbg来进行汇编语句的修改从而达到修改程序的执行结果的方法，除此之外，我还学到了修改汇编指令的时候需要寻找相应的逻辑对应的函数去寻找相应的结果的方法，我们需要找到控制的地方并且通过修改相应的函数的逻辑就可以达到相应的结果

此外，通过本实验，掌握了多个汇编语言的用法.掌握了汇编语句和函数执行时调用数据的规律。