《漏洞利用及渗透测试基础》实验报告

姓名：田晋宇　　学号：2212039　　班级：物联网班

实验名称：

OllyDBG 软件破解实验

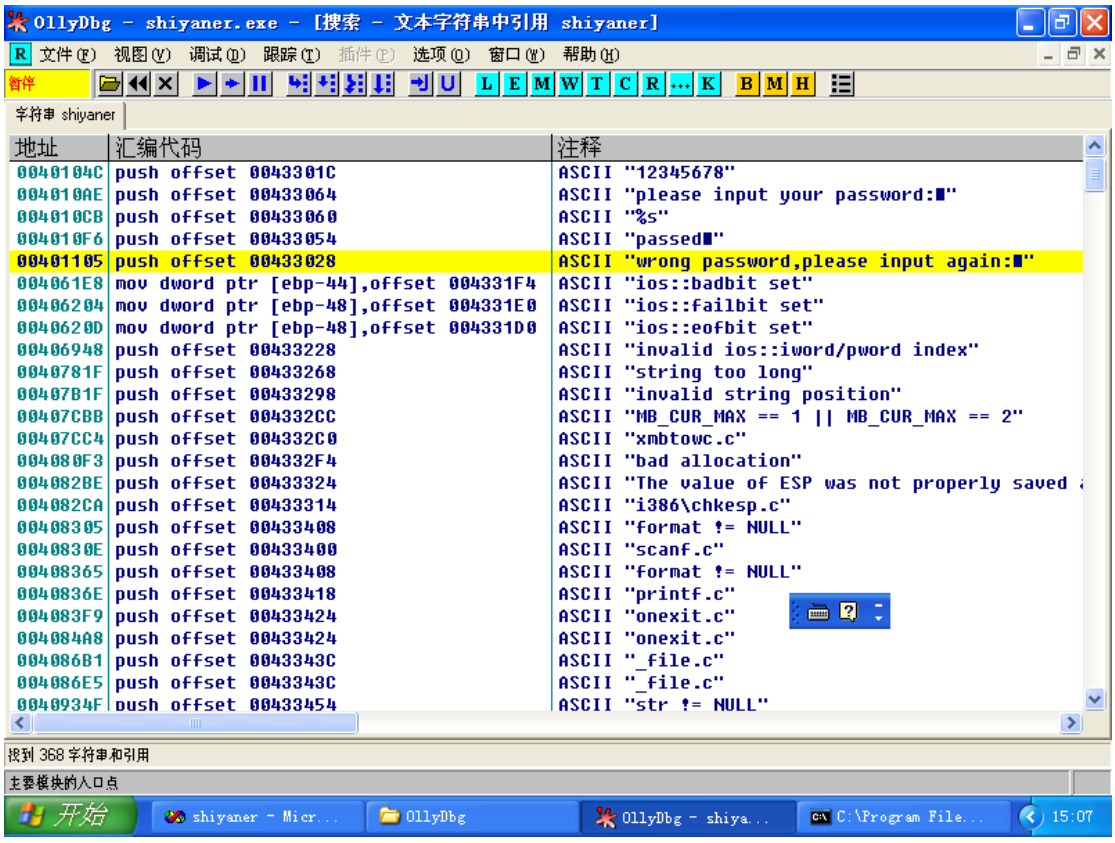
实验要求：

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。

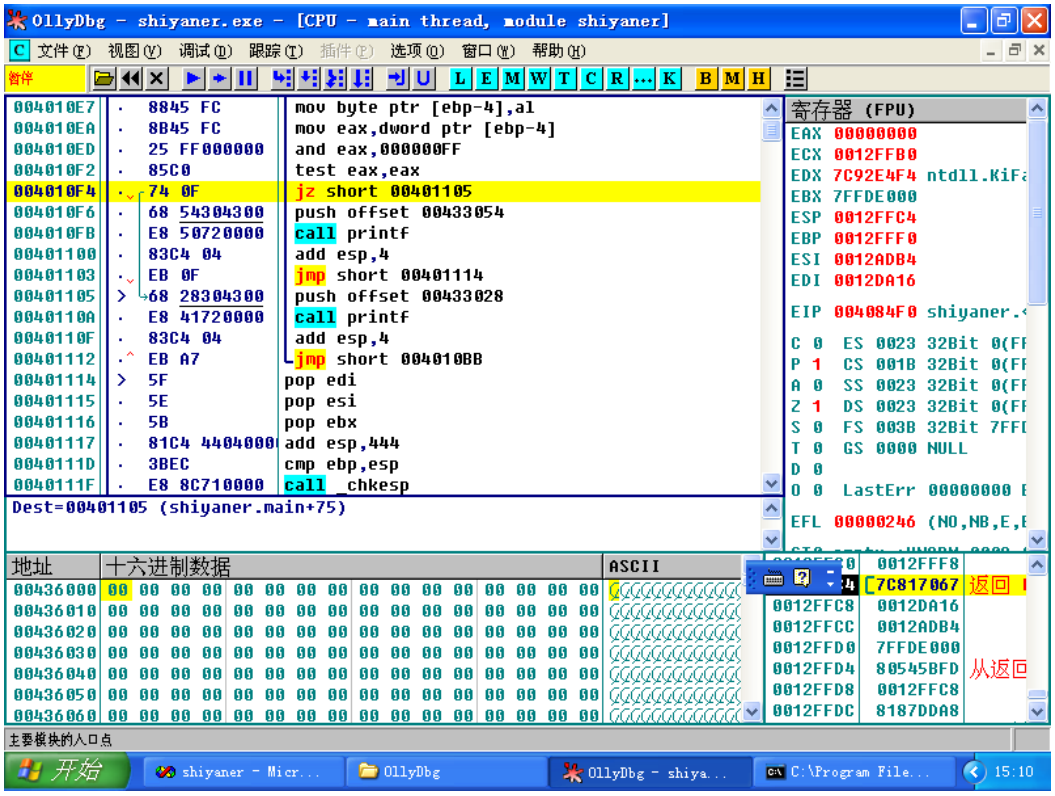
对生成的 DEBUG 程序进行破解，复现课本上提供的两种破解方法。

实验过程：

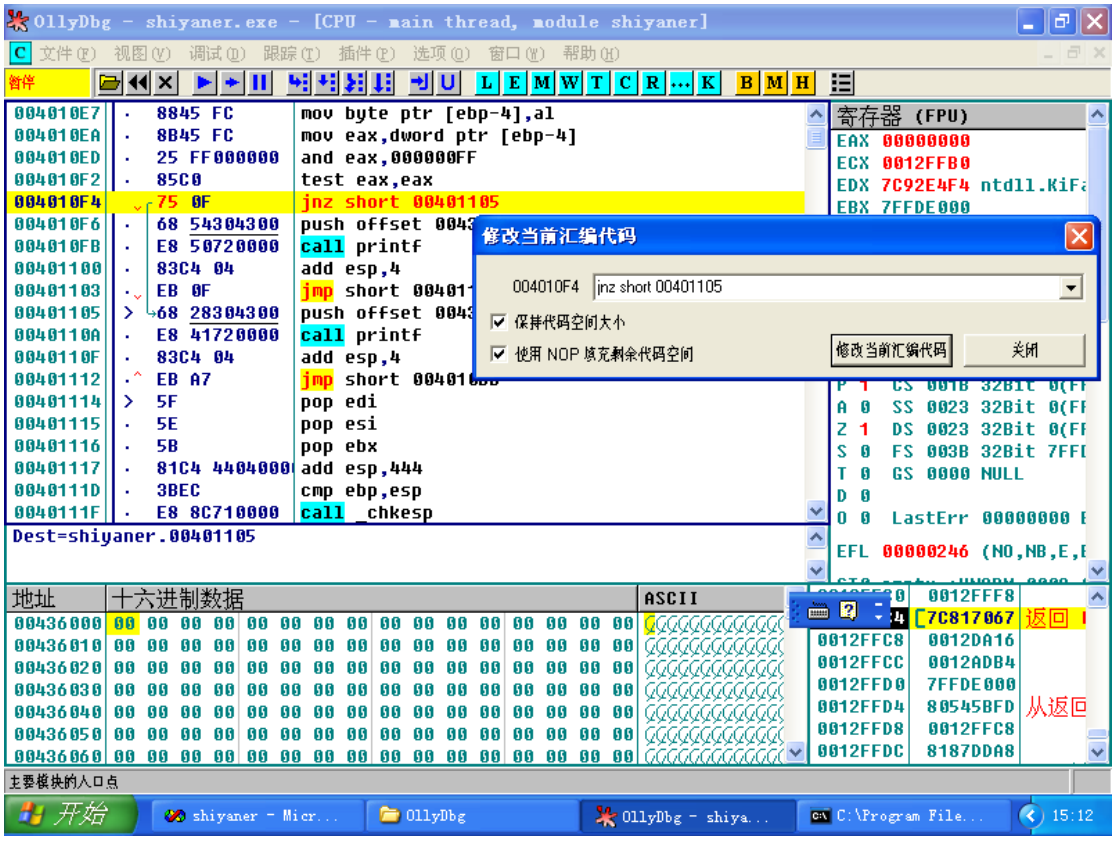
首先生成源代码的可执行程序，在 OllyDBG 中打开，进入 debug 模式，可以通过注释来找到程序的核心逻辑，当输入密码错误时，会输入 wrong password，通过查找字符串找到该命令行



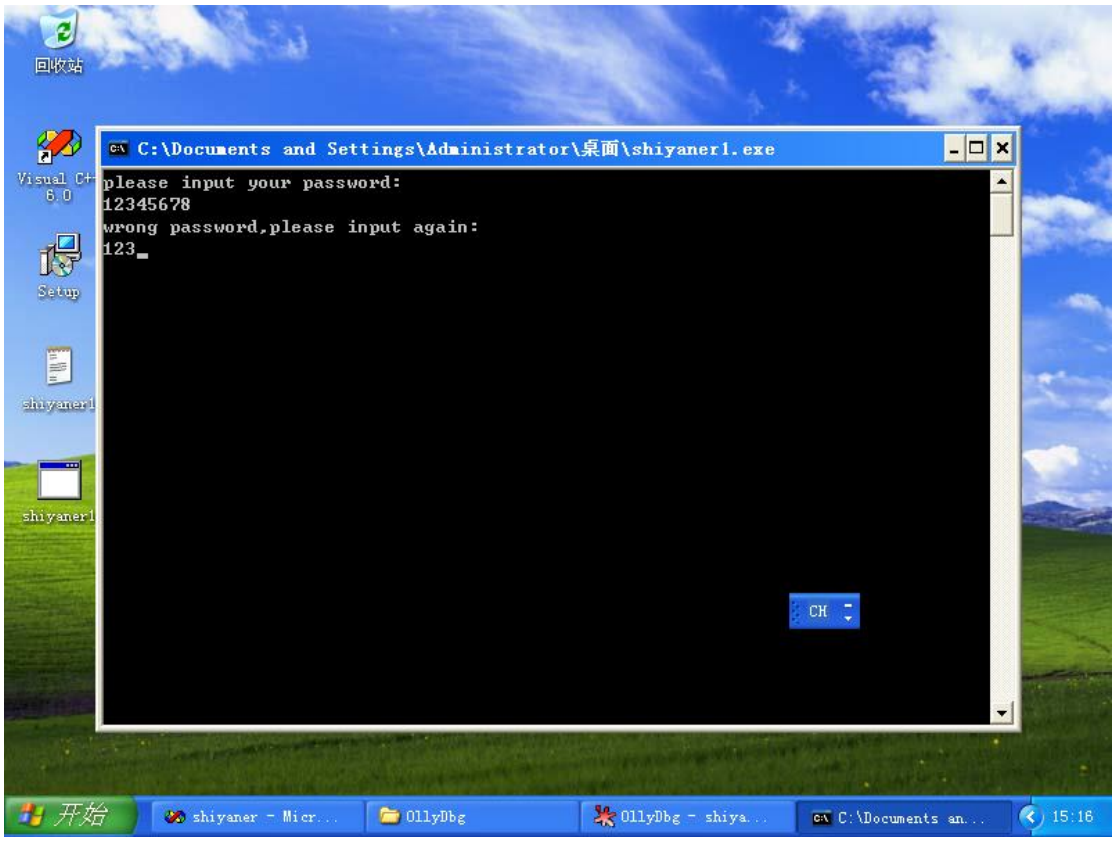
跟随到对应的汇编代码，该段通过 jz 指令进行判断，若输入错误，就会跳到密码输入错误逻辑部分



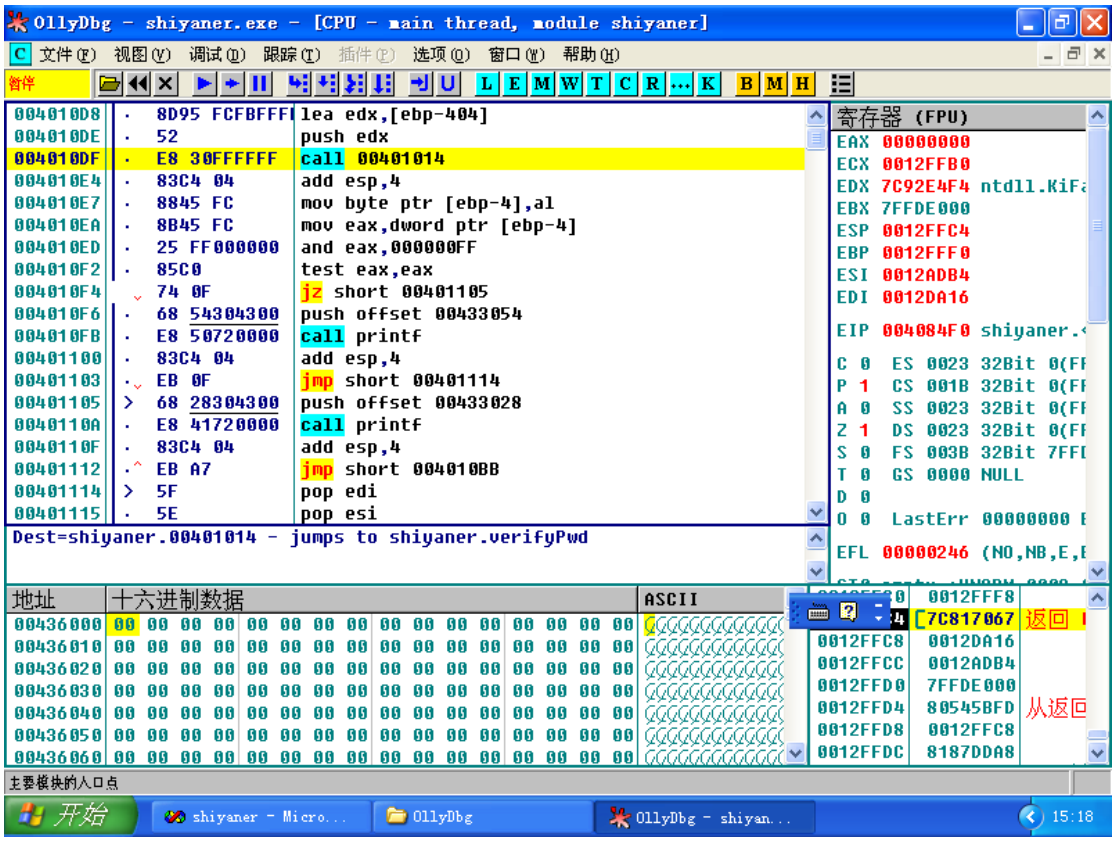
第一种破解方法就是将 jz 指令改为 jnz，改为反逻辑，即当输入密码错误时跳到输入密码正确的逻辑，完成后破解



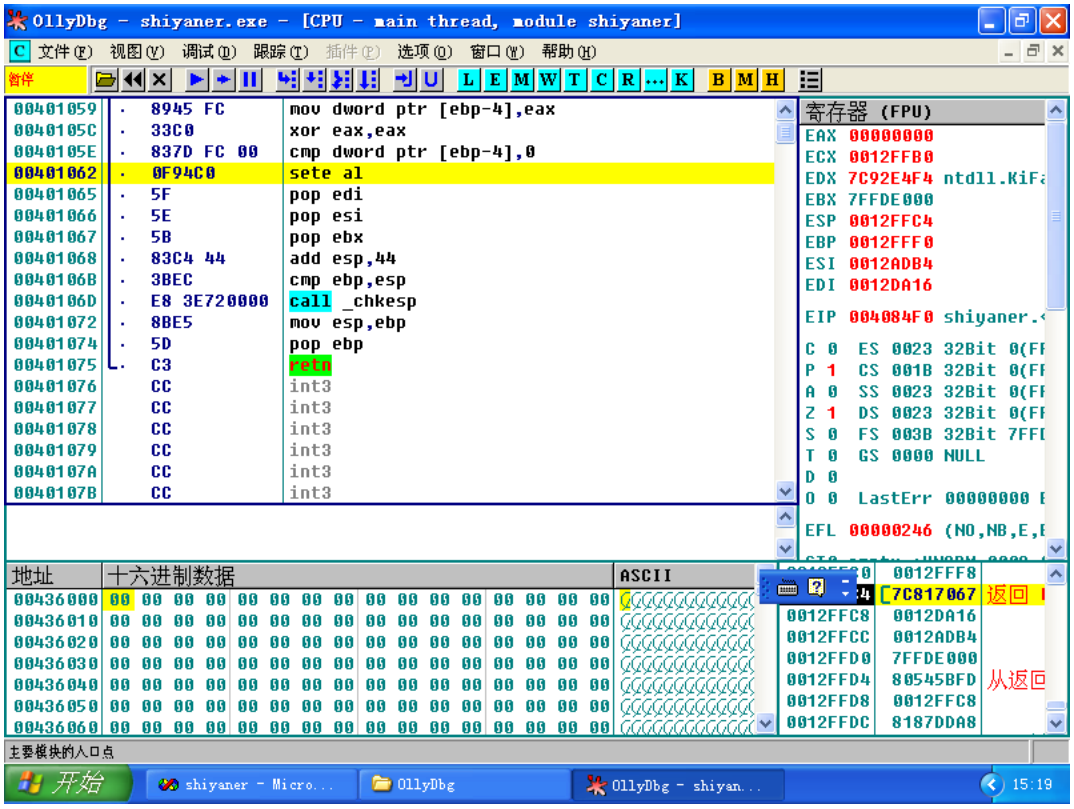
最终的效果如图，当输入密码正确时，并不会跳出程序，而输入密码错误时，程序结束



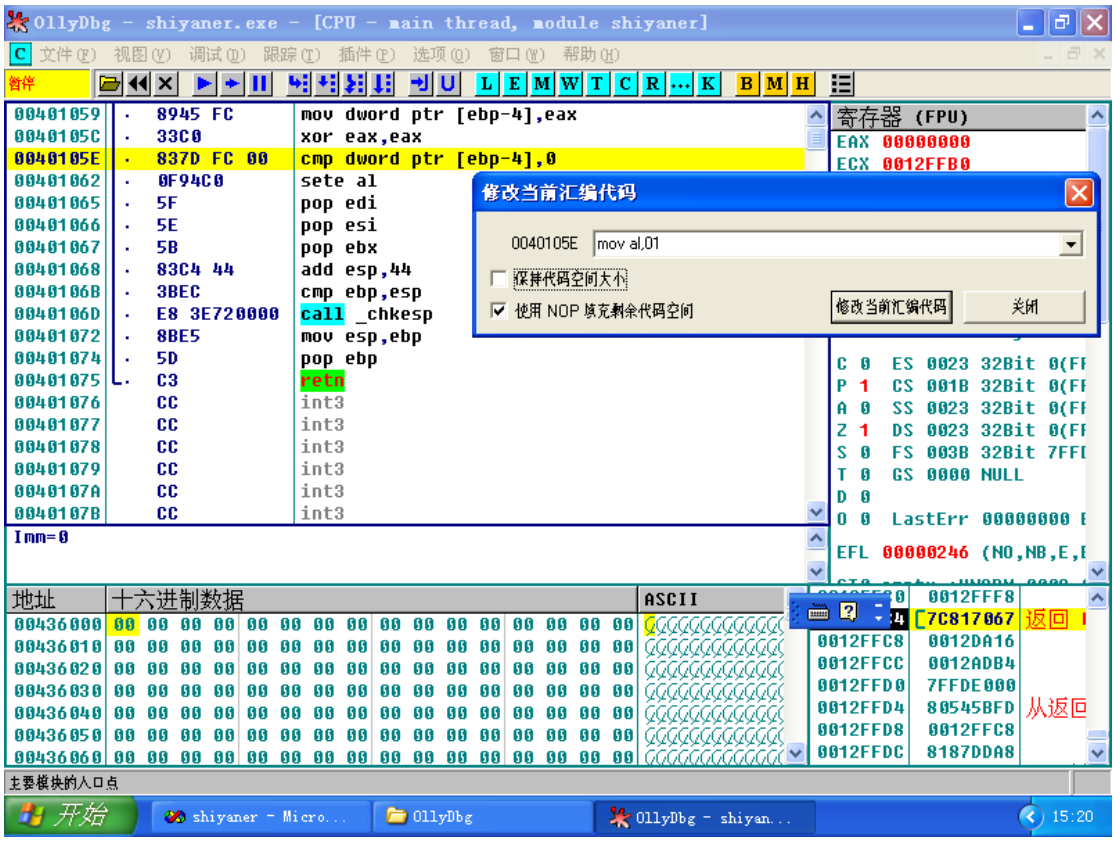
第二种破解方法的灵感来源于密码的正误由 verifyPwd 函数决定，我们找到函数的入口，跟随导函数的内部分析代码



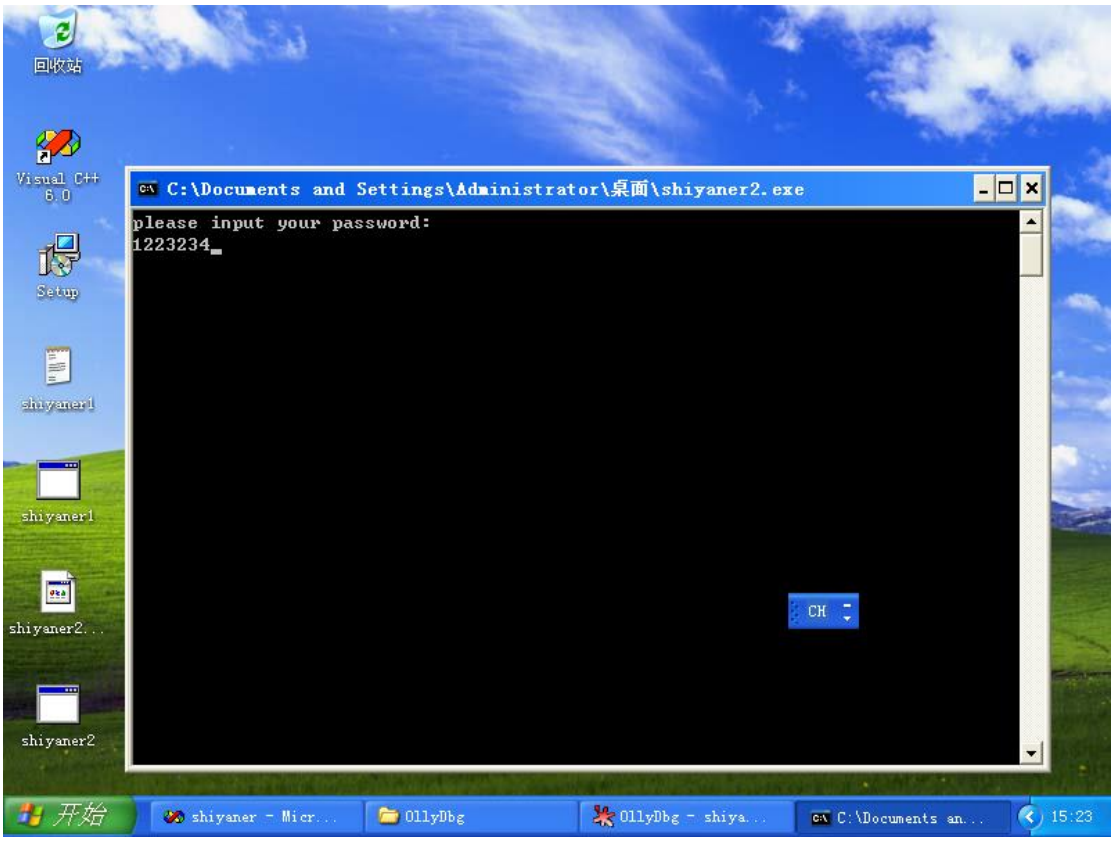
跟随到函数内部之后，我们看到一个 retn 指令，此处是函数的返回接口，我们向前找，有一 seta al 指令，此处就是该函数的返回值，因此返回值的设置就成了破解的关键



最终的效果我们希望输入任何密码都可以成功运行，我们就将 al 的值设定为 01，mov al，01，修改之后保存文件。



程序运行后吗，无论密码正确还是错误，都会跳出程序。



心得体会：

掌握了使用 OllyDBG 对软件进行破解分析，掌握 OllyDBG 的一些简单操作查找，修改，跟随等，同时加深对汇编语言的理解。