《漏洞利用及渗透测试基础》实验报告

姓名：沙璇 学号：1911562 班级：信息安全

**实验名称：**

OllyDBG软件破解

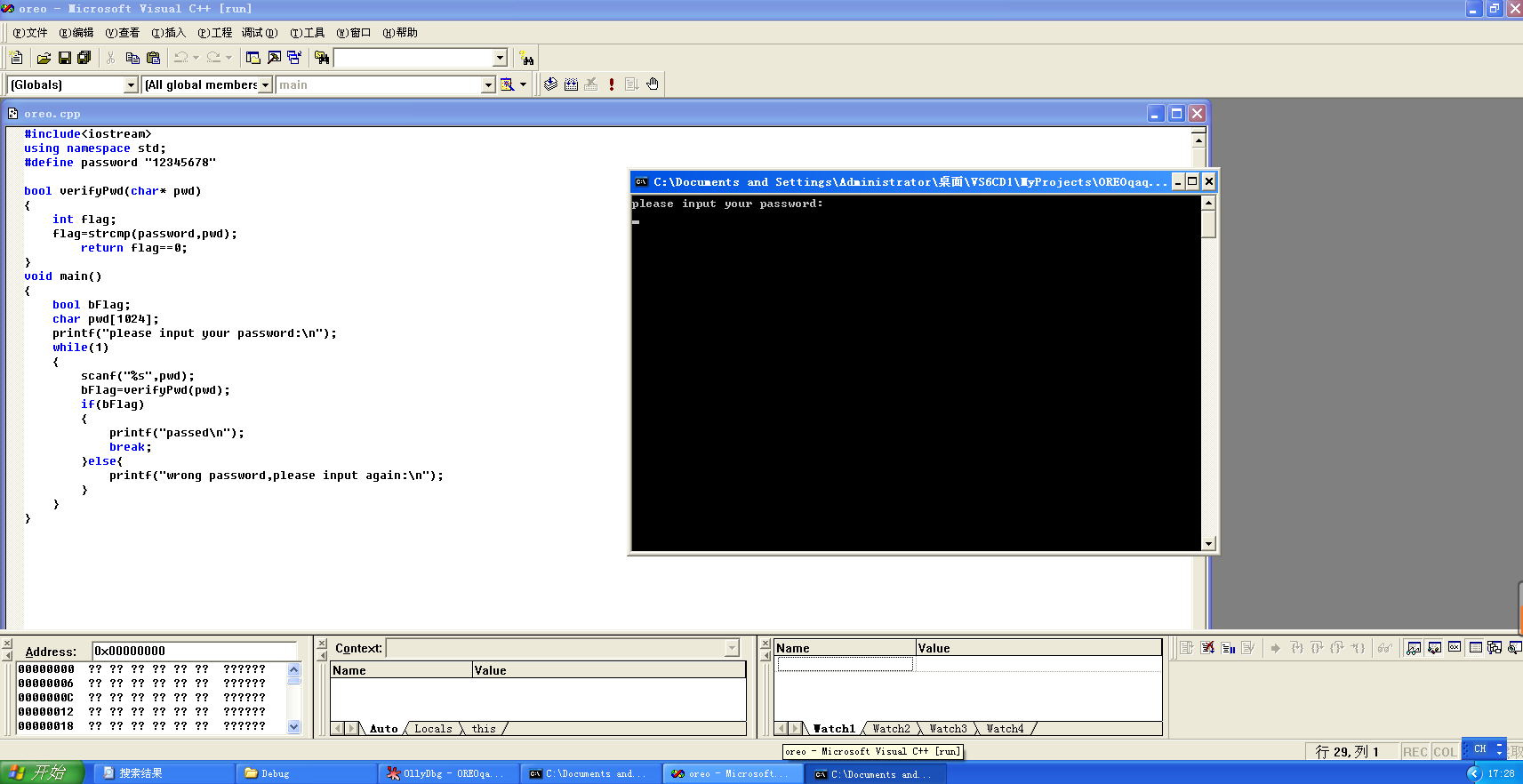
**实验要求：**

1.请在XP VC6生成课本第三章软件破解的案例（DEBUG模式，实例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。

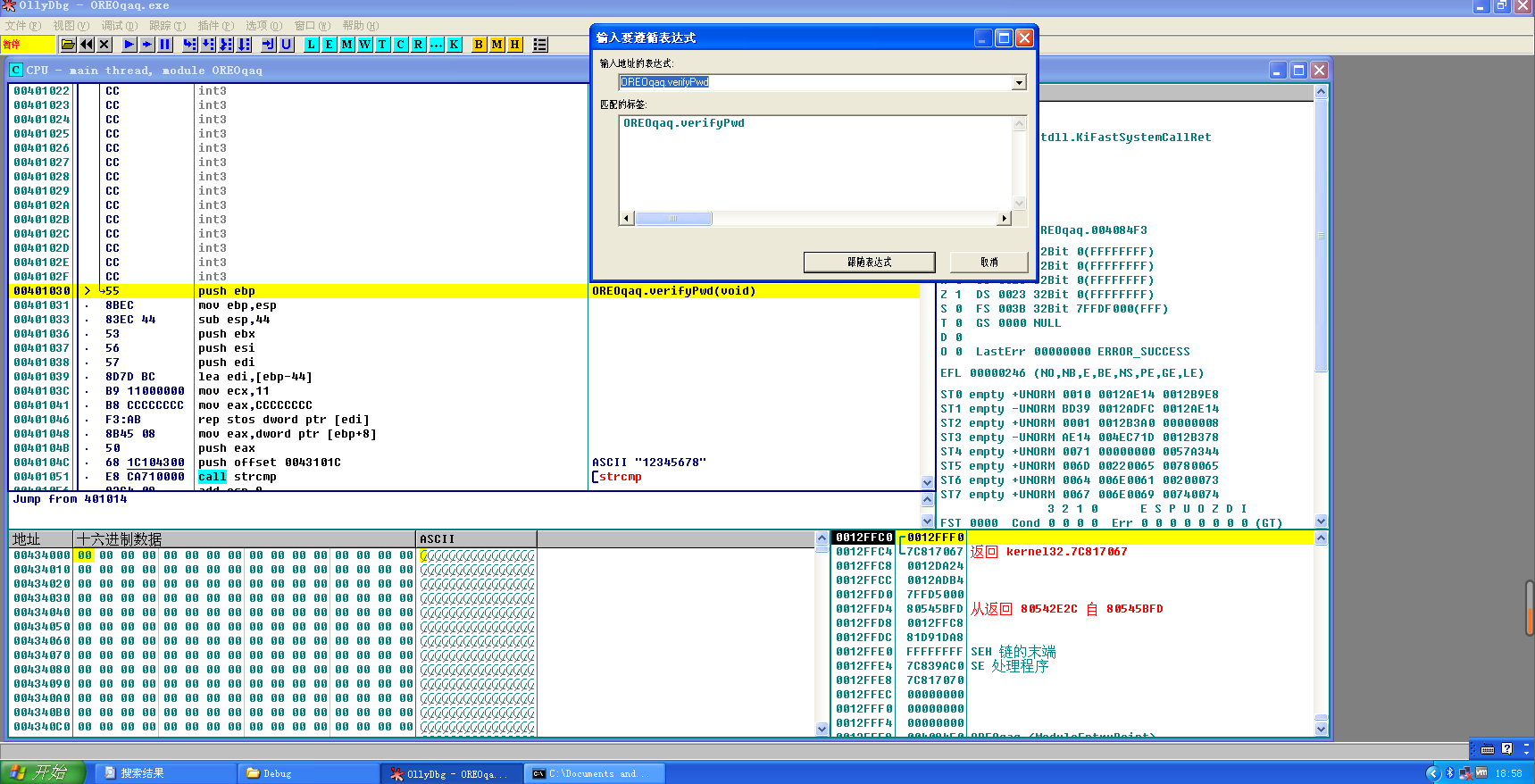
2.对生成的DEBUG程序进行破解，复现课本上提供的的两种破解方法。

**实验过程：**

**1.**在XP VC6中生成该案例并调试成功



**2.**在OllyDBG中打开该程序，右键->转到->verifypwd函数



**3.** 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。

***地址 十六进制数据 汇编代码***  ***解释***

***00401030 |> \55 push ebp***  ebp入栈

***00401031 |. 8BEC mov ebp,esp*** esp的值赋予ebp

***00401033 |. 83EC 44 sub esp,44***  esp=esp-44

***00401036 |. 53 push ebx***  ebx入栈

***00401037 |. 56 push esi***  esi入栈

***00401038 |. 57 push edi*** edi入栈

***00401039 |. 8D7D BC lea edi,[ebp-44]***  ebp-44存入edi

***0040103C |. B9 11000000 mov ecx,11***  //初始化堆栈 分配局部变量

***00401041 |. B8 CCCCCCCC mov eax,CCCCCCCC*** 拷贝数据为CCCCCCCC

***00401046 |. F3:AB rep stos dword ptr [edi]*** edi指向的区域初始化

***00401048 |. 8B45 08 mov eax,dword ptr [ebp+8]*** 从ebp+8复制到eax

***0040104B |. 50 push eax***  eax入栈

***0040104C |. 68 1C104300 push offset 0043101C***  压入字符串偏移地址

***00401051 |. E8 CA710000 call strcmp***  调用strcmp函数

***00401056 |. 83C4 08 add esp,8***  esp=esp+8

***00401059 |. 8945 FC mov dword ptr [ebp-4],eax***  将eax的值存入ebp-4

***0040105C |. 33C0 xor eax,eax***  清零

***0040105E |. 837D FC 00 cmp dword ptr [ebp-4],0***  比较0与ebp-4的值

***00401062 |. 0F94C0 sete al***  cmp执行后，相等置零

***00401065 |. 5F pop edi***  释放edi

***00401066 |. 5E pop esi***  释放esi

***00401067 |. 5B pop ebx***  释放ebx

***00401068 |. 83C4 44 add esp,44***  esp=esp+44

***0040106B |. 3BEC cmp ebp,esp***  比较ebp与esp

***0040106D |. E8 3E720000 call \_chkesp***  调用chkesp函数

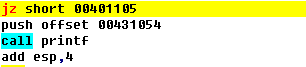
***00401072 |. 8BE5 mov esp,ebp***  ebp的值赋予esp

***00401074 |. 5D pop ebp***  释放ebp

***00401075 \. C3 retn***  释放eip

4.复现破解方法：

*a.破解方法1：*



找到关键跳转代码，注意到为0时跳转到错误分支，那么将jz改为jnz，为0时则转入正确分支。



保存更改后，输入错误密码时程序顺利执行。

复现成功！

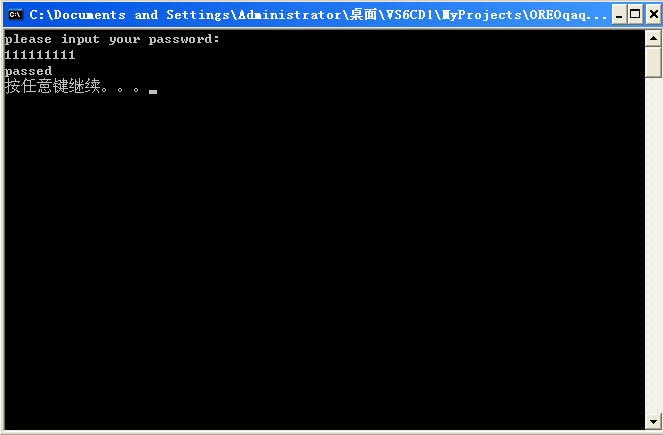
*b.破解方法2：*



注意到verityPwd函数内部关键比较代码。当比较后的值为0(即输入正确)时，ZF标志位为1，al的值为1。那么不进行比较，直接将al赋值为1。



保存更改后，输入错误密码时：



复现成功！

**心得体会：**

加强了对汇编语言的了解，进一步熟悉了OllyDBG的使用方法，对破解应用程序有了初步的认知和了解。