《软件安全》实验报告

姓名：辛浩然　　学号：2112514　　班级： 信息安全、法学

实验名称：

OllyDBG 破解实验

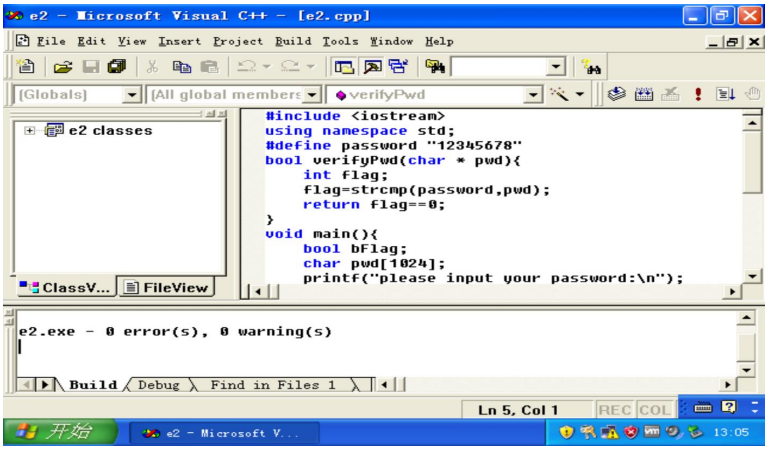
实验要求：

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。

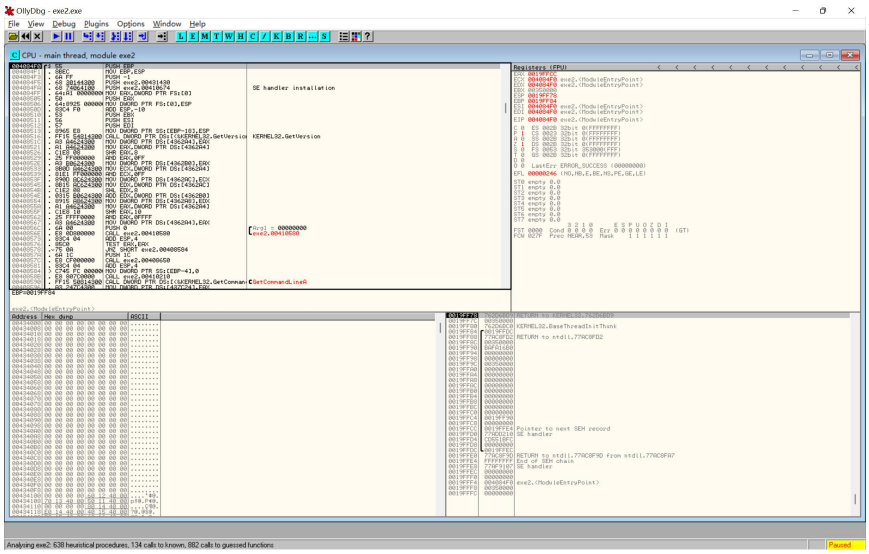
2.对生成的 DEBUG 程序进行破解复现课本上提供的两种破解方法，

实验过程：

1.生成 Debug 模式的 exe 程序。



2.在 OllyDBG 中打开 exe 程序。



3. 单步调试，获取 verifyPWD 函数对应的汇编代码

```
00001030  55              PUSH EBP
00001031  8BEC            MOV EBP,ESP
00001033  83EC 44         SUB ESP,44
00001036  53              PUSH EBX
00001037  56              PUSH ESI
00001038  57              PUSH EDI
00001039  8D7D BC         LEA EDI,DWORD PTR SS:[EBP-44]
0000103C  B9 11000000     MOV ECX,11
00001041  B8 CCCCCCCC     MOV EAX,CCCCCCCC
00001046  F3:AB           REP STOS DWORD PTR ES:[EDI]
00001048  8B45 08         MOV EAX,DWORD PTR SS:[EBP+8]
0000104B  50              PUSH EAX
0000104C  68 1C104300     PUSH 43101C
00001051  E8 CA710000     CALL 00008220
00001056  83C4 08         ADD ESP,8
00001059  8945 FC         MOV DWORD PTR SS:[EBP-4],EAX
0000105C  33C0            XOR EAX,EAX
0000105E  837D FC 00      CMP DWORD PTR SS:[EBP-4],0
00001062  0F94C0          SETE AL
00001065  5F              POP EDI
00001066  5E              POP ESI
00001067  5B              POP EBX
00001068  83C4 44         ADD ESP,44
0000106B  3BEC            CMP EBP,ESP
0000106D  E8 3E720000     CALL 000082B0
00001072  8BE5            MOV ESP,EBP
00001074  5D              POP EBP
```

其中对应 flag==0 的汇编代码：

mov dword ptr ss:[ebp-4],eax

将 strcmp 函数调用后的返回值（存在 eax 中）赋值给变量 flag

xor eax,eax

将 eax 值清空

cmp dword ptr ss:[ebp-4],0

将 flag 的值与 0 进行比较，即 flag==0

sete al

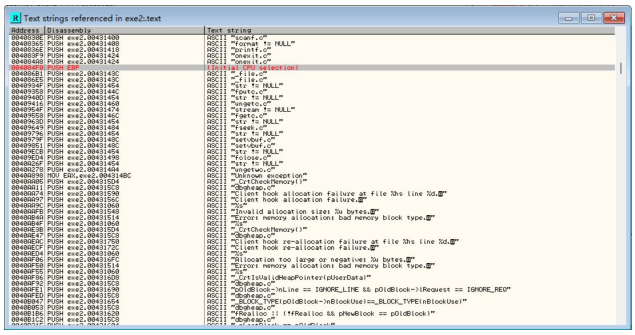
sete 是根据状态寄存器的值，如果相等则设置，如果不相等则不设置

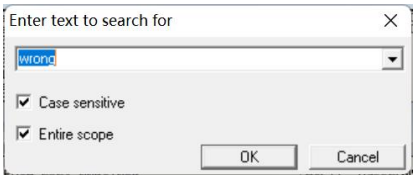
4.破解方法复现

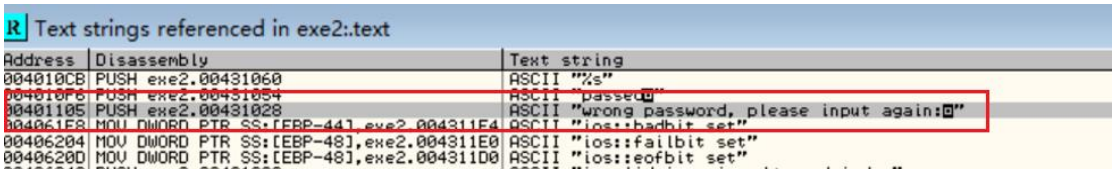
（1）破解方式一

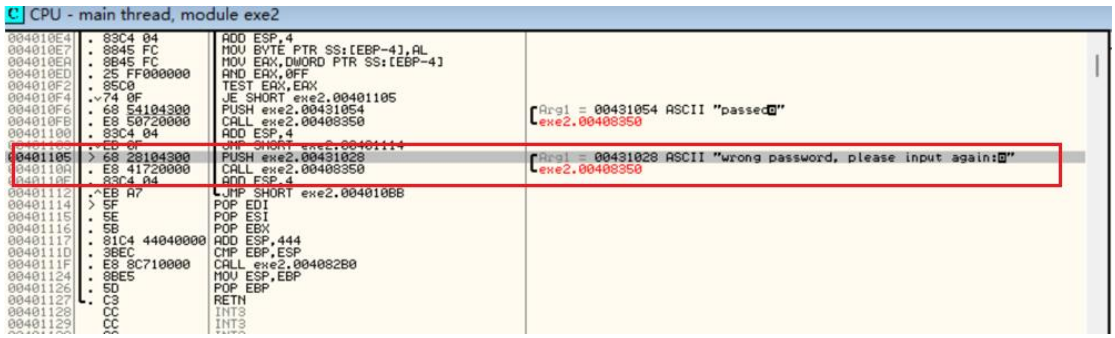
首先打开“所有引用的字符串”，通过查找“wrong”定位出错信息的代码，

并定位在反汇编代码中。







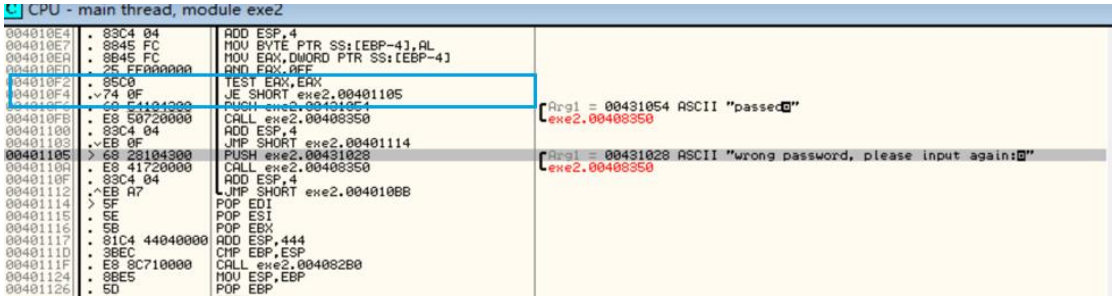


观察反汇编代码，可以找到输入密码的条件判断语句：

test eax,eax

je 00401105

如果输入密码错误，则跳转至 00401105 地址处，输出错误信息。

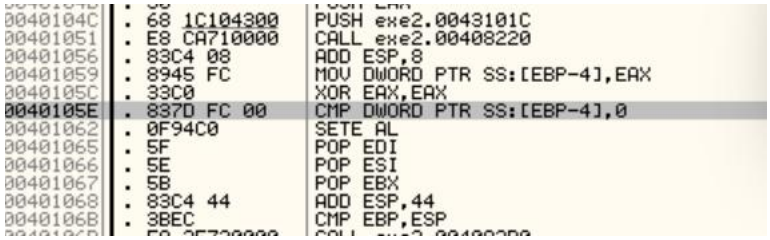


对其进行修改，将跳转判断 je 00401105（相等跳转）修改为 jnz 00401105（不相等跳转），以阻止输入错误而输出错误信息。

将修改复制到可执行文件后，即可完成破解。

（二）破解方式二

进入 verifyPwd 函数



cmp dword ptr ss:[ebp-4],0

将 flag 的值与 0 进行比较，即 flag==0。

sete al

sete 是根据状态寄存器的值，如果相等则设置，如果不相等则不设置。

由上述代码分析可知，flag==0 时，密码正确，al 置为 1。既然这样，可以直接修改 al，使其值恒为 1。

将 cmp dword ptr ss:[ebp-4],0 修改为 mov al,1，用 nop 空指令填充。

将修改复制到可执行文件后，即完成破解，无论密码输入正确与否，都将通过。

心得体会：

1.通过实验，掌握 OllyDBG 的基本操作；

2.通过复现破解操作体会到逆向分析与程序破解的基本方法与思想；

3.对汇编语言一些语句的含义与用法的理解更为深入。