《软件安全》实验报告

姓名：刘星宇　　学号：2212824　　班级：信息安全法学双学位班

实验名称：

IDE 反汇编实验

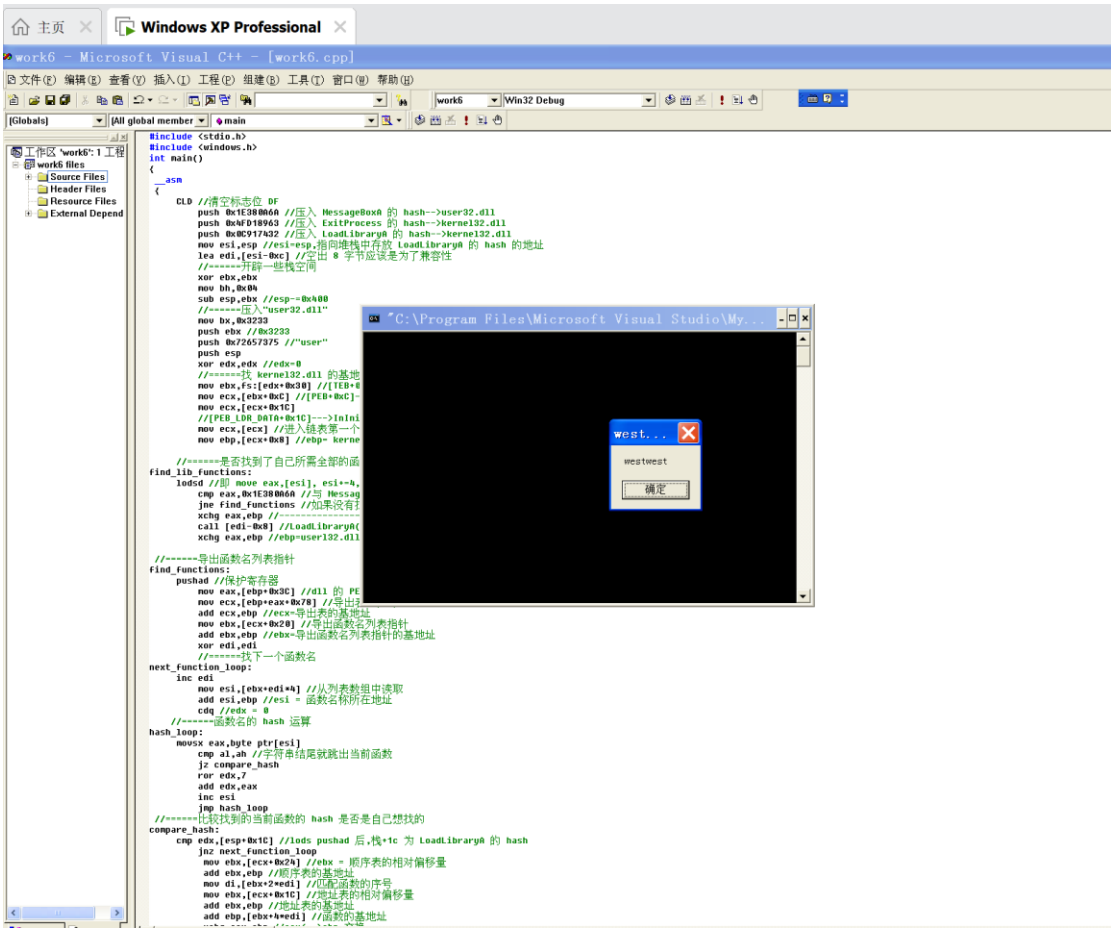
实验要求：

实验要求:

复现第五章实验七,基于示例 5-11,完成 API 函数自搜索的实验,将生成的 exe 程序,复制到 windows 10 操作系统里验证是否成功。

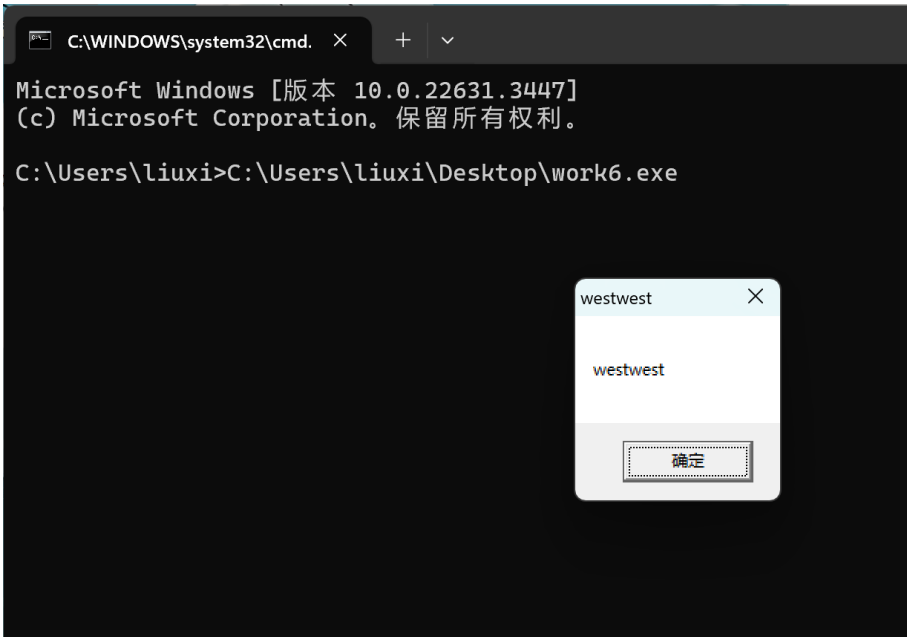
实验过程：

1. 复现 5-11 ， 完成 API 自搜索实验。



~~~~~~~

2. 将生成的 exe 程序,复制到 windows 10 操作系统里验证
~~~~~~~



验证成功。

心得体会：

基于示例 5-11 进行实验，这个过程让我对 API（应用程序编程接口）和其在程序中的动态搜索与加载机制有了更为清晰的认识。

API 是软件应用程序之间的通信协议，它定义了一套规则和方法，使得不同的软件组件可以相互调用彼此的功能。API 通常以函数、协议和工具的形式存在，为开发者提供了与特定软件服务或资源交互的能力。

在实验中，我认识到 API 自搜索函数的核心目的是在不直接引用 API 函数地址的情况下，通过某种机制在内存中搜索并定位到所需的 API 函数地址。这种机制在反病毒、反调试和某些系统级编程中非常有用。

API 自搜索函数通常利用 Windows PEB（进程环境块）或 Kernel32.dll 等模块的基地址，结合 API 函数的相对偏移量来定位其实际地址。这种机制允许程序在运行时动态地解析 API 函数的地址，从而提高了程序的灵活性和适应性。

通过这次对 API 自搜索函数的研究和实验，我对 API 的工作原理和动态加载机制有了更为深入的理解。