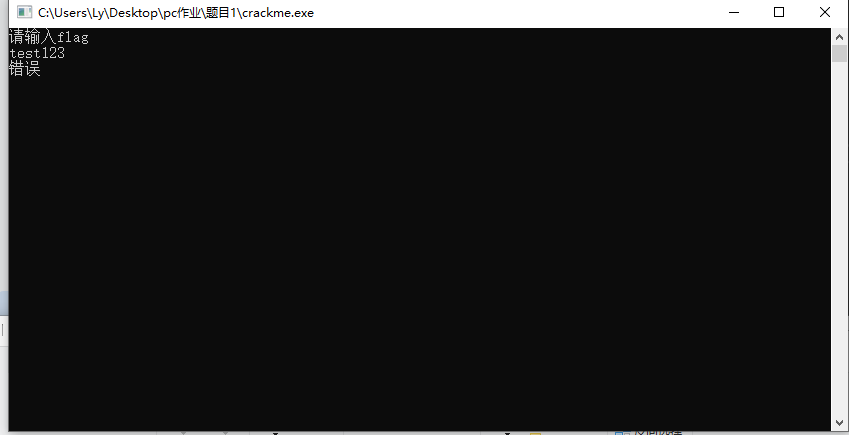
菁英班PC端作业题目说明

一、基本信息

本次作业提供一个Windows端可直接运行的exe文件

|  |  |
| --- | --- |
| 文件名 | MD5 |
| crackme.exe | 76f8e38b3bcb8ccaecd33c5e65b80e50 |

管理员模式运行 crackme.exe ，控制台会提示输入flag字符串，输入后并回车，程序会校验flag是否正确并在控制台输出结果



二、环境要求

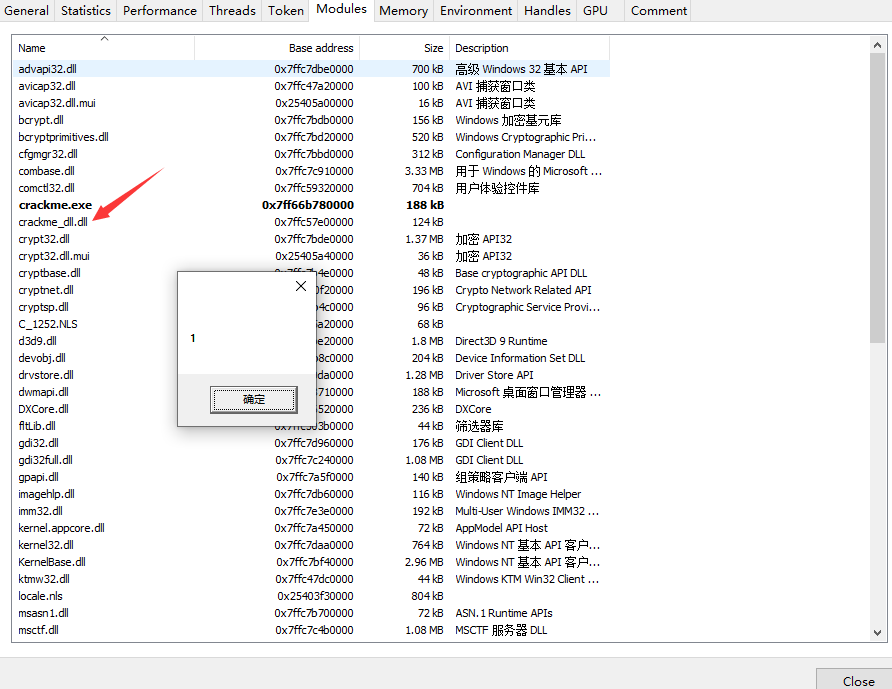
请在Win10/Win11 系统分析调试

三、题目要求

1. **远程注入**模块

使用Windows API CreateRemoteThread 远程注入模块到crackme进程中并且不崩溃，然后使用ark工具(例如processhacker等)能够查看注入模块的信息。

(示例图)



1. **分析并调试程序**，找到正确的flag
2. 利用注入的DLL ，Hook程序代码

**通过Hook进程中的函数使得输入任何字符串，控制台都会打印”正确”**。