### 一、编程题（2道\*25分）

1.输入 n 个整数，找出其中的最大值和最小值。

2.输入一个整数，计算并输出它的阶乘。

### 二、程序分析题（2道\*20分）

3.

#include <stdio.h>

#include <string.h>

#include <stdlib.h>

int main() {

char buffer[1024];

strcpy(buffer, "Hello, UDP!");

printf("Sending: %s\n", buffer);

return 0;

}

Sending：Hello, UDP!

### 三、简答题（1道\*10分）

解释 XSS 攻击的类型及其防范措施。

XSS可分为，反射型（你给别人发个链接，需要别人点一下，），存储型（评论区），DOM型

XSS（Cross-Site Scripting）是一种前端攻击，攻击者通过向网页注入恶意脚本，使用户在访问该网页时执行攻击代码，可能导致 **用户数据泄露、劫持会话、网页篡改** 等后果。

**🔹 XSS 的三种类型**

**① 反射型 XSS（Reflected XSS）**

**特点：**

**恶意代码不存储在服务器**，而是通过 URL 参数、表单提交等方式传递。

需要**诱导受害者点击**恶意链接后，代码才会执行。

 **对用户输入进行过滤和转义**（如将 < 转换为 &lt;）。

 **使用 CSP（内容安全策略）**，限制脚本的来源。

 **避免在 HTML 中直接拼接用户输入**，而是用安全的 API（如 innerText）。

**② 存储型 XSS（Stored XSS）**

**特点：**

* **恶意代码存储在服务器**，所有访问该页面的用户都会受到影响。
* 常见于**评论区、论坛、博客等存储用户输入的地方**。

** 存储前对用户输入进行 HTML 实体编码（< → &lt;）。**

** 严格限制可输入的内容（如 Markdown 解析器、富文本编辑器的安全过滤）。**

** 使用 HTTPOnly Cookie，防止 JavaScript 访问 Cookie。**

③ DOM 型 XSS（DOM-Based XSS）

特点：

发生在浏览器端，不依赖服务器的响应，而是 JavaScript 代码在客户端动态修改 DOM 结构导致的攻击。

常见于 innerHTML、document.write() 等 API 直接插入用户输入数据的情况。

 **避免使用 innerHTML，改用 textContent 或 innerText。**

 **使用安全 API（如 DOMPurify 库）清理不可信输入。**

 **限制 URL 参数的输入格式**，如 正则匹配 仅允许合法字符。

解释 ICMP 协议的作用，并分析 ping 命令的工作原理

1.ICMP为网际控制报文协议，属于网络层协议，属于TCP/IP体系，主要功能是允许主机报告错误信息以及询问信息，ICMP主要有两种报文，一种为差错报告报文，如时间超时，终点不可达，参数问题，改变路由，应用实例有traceroute.(时间超时、终点不可达)一种是ICMP询问报文，如回送请求和回送回答以及时间戳回答，如Ping(回送请求与回送回答)。

针对一些错误报文不回送差错报告报文，1.ICMP差错报文本身2.第一个分片的数据报回送了，后续就不回送了，多播数据报不回送，特殊地址（127.0.0.0/0.0.0.0）不回送。