计算机网络实验四 Wireshark 抓包实例分析

浮焕然 PB22061345

一、思考题

1. 解释 HTTP 中的幂等是什么意思（可以联想一下线性代数里的矩阵的意义以及幂等矩阵）?

HTTP 中的幂等（Idempotence）是指一个操作，不论执行多少次，其结果都是相同的。也就是说，多次执行一个幂等操作，和只执行一次的效果是一样的，不会改变资源的状态。

这个概念类比于线性代数中的幂等矩阵。在矩阵理论中，一个方阵如果与其自身的乘积等于它自己，那么这个矩阵就被称为幂等矩阵。用数学表达式表示就是，如果矩阵 A 满足$\mathbf{A}^2 = \mathbf{A}$，那么 A 就是一个幂等矩阵。

2. GET 操作是幂等的吗, POST 呢?

GET	在 HTTP 协议中，GET 请求用于从服务器检索数据。GET 操作是幂等的，这意味着无论你执行多少次 GET 请求，它都不会改变服务器上的数据或资源状态。多次执行相同的 GET 请求，服务器的状态保持不变，返回的结果也相同。
POST	POST 请求用于向服务器提交数据，通常用于创建新的资源或引发服务器上的状态变化。由于 POST 操作可能会改变服务器的状态，因此它通常不是幂等的。如果你多次执行相同的 POST 请求，可能会导致服务器上创建多个资源或引发多次状态变化，这与幂等性的定义相违背。

3. HTTPS 抓到的数据包与之前 HTTP 中抓到的有何不同, 这是什么原因导致的?

不同: HTTPS 抓包的都是已加密内容, 不能直接读取, 而 HTTP 则可以直接读取其中的内容。

原因:

HTTPS 抓到的数据包与 HTTP 抓到的数据包的主要区别在于加密和安全性。HTTPS 通过 SSL/TLS 协议对传输的数据进行加密，这使得数据在传输过程中是安全的，不易被窃取或篡改。而 HTTP 协议以明文方式发送内容，不提供任何方式的数据加密，因此安全性较差，如果攻击者截取了传输报文，就可以直接读懂其中的信息。

此外，HTTPS 默认使用 443 端口，而 HTTP 默认使用 80 端口。HTTPS 还提供了身份验证机制，通过数字证书验证服务器的身份，防止中间人攻击和伪装。

4. 解释从输入网址, 到浏览器显示网页, 在应用层依次发生了什么?

步骤如下：

解析网址	浏览器首先解析输入的 URL，确定协议（如 HTTP 或 HTTPS）、域名、端口（如果指定）和路径
DNS 解析	浏览器需要将域名转换为 IP 地址，这通过 DNS（域名系统）查询完成。如果域名已经在本地 DNS 缓存中，浏览器将直接使用缓存的 IP 地址；否则，它将向 DNS 服务器发送查询请求
建立连接	一旦有了 IP 地址，浏览器会通过传输层（通常是 TCP）建立到服务器的连接。对于 HTTPS，这个连接将被加密
发送 HTTP 请求	连接建立后，浏览器会构建一个 HTTP 请求，包括请求方法（如 GET 或 POST）、请求头（包含用户代理、接受的内容类型等信息）和请求体（如果适用）
服务器处理请求	服务器接收到请求后，会根据请求的 URL 和方法来处理请求。这可能包括查询数据库、执行脚本、调用 API 等
生成 HTTP 响应	服务器处理完请求后，会生成一个 HTTP 响应，包括状态码（如 200 表示成功）、响应头（如内容类型、内容长度等）和响应体（即网页内容）
浏览器接收响应	浏览器接收到服务器的响应后，会解析状态码和响应头，然后根据内容类型（如 HTML、CSS、JavaScript、图片等）来处理响应体
渲染网页	浏览器开始解析 HTML 文档，构建 DOM（文档对象模型）树。同时，它会解析 CSS 并构建 CSSOM（CSS 对象模型）。然后，浏览器将 DOM 和 CSSOM 合并成渲染树，并计算每个元素的布局（即回流）
执行 JavaScript	如果网页包含 JavaScript，浏览器会解析并执行这些脚本。JavaScript 可以动态修改 DOM 和 CSSOM，这可能会导致浏览器重新计算布局和重绘页面
加载资源	浏览器会根据 HTML 中的引用（如图片、视频、音频、CSS 文件、JavaScript 文件等）并行加载这些资源。这些资源的加载可能会触发额外的 HTTP 请求
完成加载	一旦所有资源都加载并处理完毕，浏览器会显示完整的网页

二、总结

1. Internet 以 TCP/IP 模型为基础进行构建，依托操作系统的核心协议栈。
2. 从 Internet 协议栈的角度看，自顶向下依次可以分为应用层，传输层，网络层，网络接口层（ 数据链路层与物理层 ）。
3. 从计算机系统的角度看，应用层运行于用户空间中，传输层，网络层，网络接口层运行于操作系统中. Internet 网络通过对不同功能进行整合分层，利用协议指定各层的交互规范，配合各层之间的接口通信，实现对外界的完整服务功能。
4. 超文本传输协议（HyperText Transfer Protocol, HTTP）是互联网上应用最为广泛的一种网络传输协议. HTTP 协议通过统一资源定位器（URL）来标识服务器上的资源，客户端可以向这个 URL 发送 HTTP 请求报文（Request Messages），服务端根据情况返回响应报文。
5. 超文本传输安全协议（HyperText Transfer Protocol over Secure Socket Layer, HTTPS）是一种通过计算机进行安全通信的应用层传输协议. HTTPS 利用标准的 HTTP 协议进行数据通信，采用传输层安全协议 SSL/TLS（Socket Secure Layer/Transport Layer Security）来对数据包提供机密性与完整性服务，同时对客户端与服务器的合法性进行认证。
6. 域名系统（Domain Name System, DNS) 是一项用于网络域名管理的互联网服务. 它作为将域名和 IP 地址相互映射的一个分布式数据库，能够使人更方便地访问互联网. DNS 使用 TCP 和 UDP 端口 53.
7. DNS 采用层次化的名字空间，每个层次都有多个名字，每个名字对应着一个域，这些名字也被称为域名. 域名由定义该层及以其上层名字的字符串组成，不同层的字符串用“.”隔开
8. 文件传输协议（File Transfer Protocol, FTP）是一个用于在计算机网络上在客户端和服务器之间进行文件传输的应用层协议. 一般运行在 20 和 21 两个端口，端口 20 用于在客户端和服务器之间传输数据流，而端口 21 用于传输控制流
9. FTP 有两种使用模式：主动模式和被动模式
   主动模式要求服务端主动向客户端建立数据连接. 在这种情况下，客户端的防火墙可能拦截服务端的连接建立请求. 因此增加了被动模式，被动模式中服务端被动接收客户端的连接建立请求，从而绕过客户端的防火墙

被动模式的通信流程	主动模式的通信流程