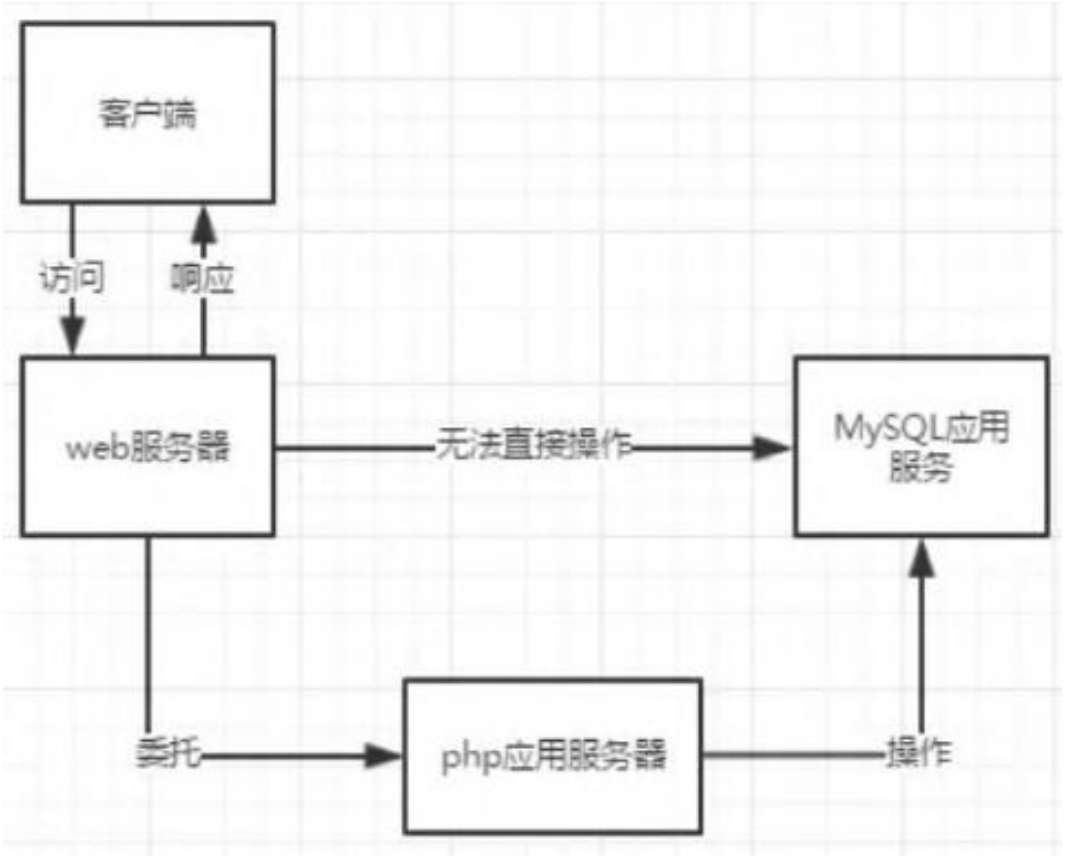
计算机网络攻防实验课

第9周

陈健

chenj@nju.edu.cn

Web攻防简介：浏览器访问网站



常见的Web服务器

- Apache HTTP Server
- Nginx
- IIS
- Lighttpd
- Tomcat

Web前端语言

- HTML：超文本的标记语言
- CSS：层叠样式表
  - 一种用来表现HTML或XML等文件样式的计算机语言
- JavaScript
  - 一种可以插入HTML页面，可以由绝大多数现代浏览器执行的轻量级的编程语言。
  - 对前端安全非常重要

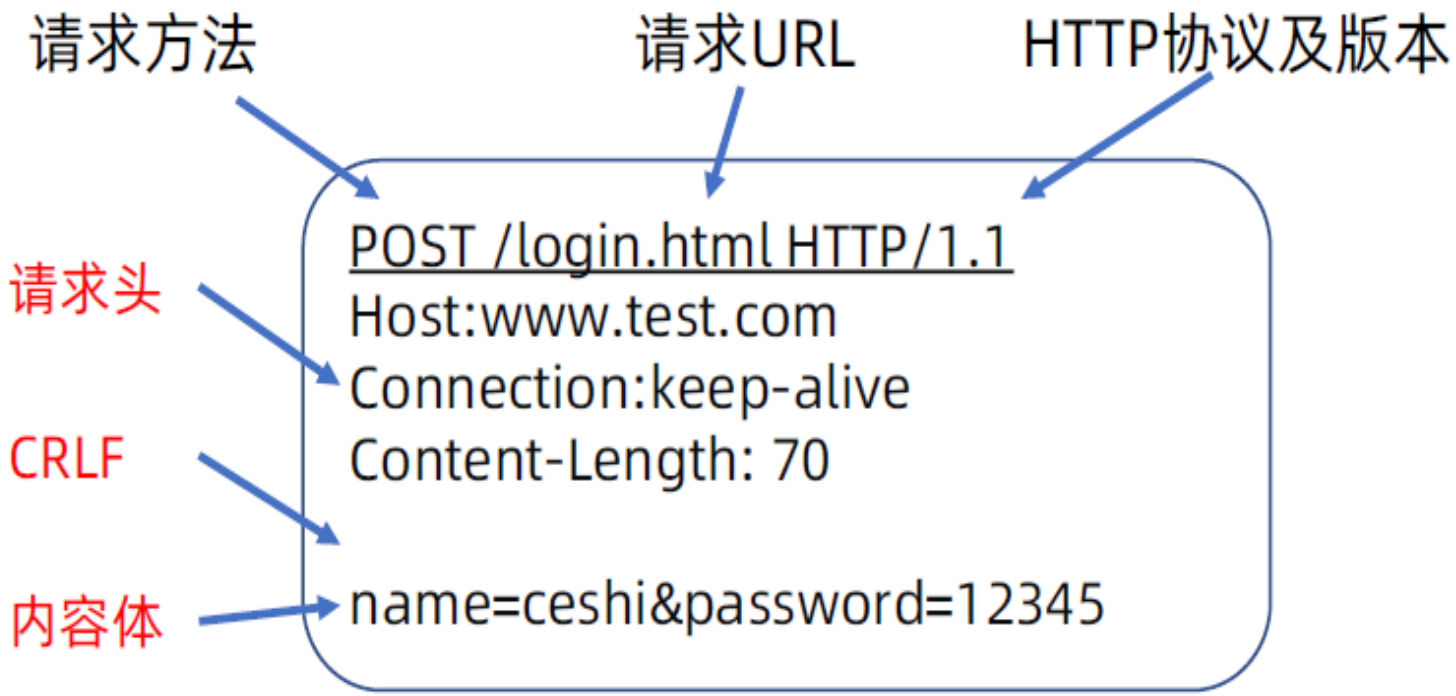
Web应用框架

- Web应用框架（Web application framework）是一种开发框架，用来支持动态网站、网络应用程序及网络服务的开发。
- 前端流行框架
  - jQuery、Bootstrap、React.js、Vue等
- 后端流行框架
  - Spring MVC、Django、Flask、Tornado等

HTTP协议

- HTTP协议定义了Web客户端如何从Web服务器请求Web页面，以及服务器如何把Web页面传送给客户端
  - 一个HTTP客户端，通常是浏览器，与Web服务器的HTTP端口（默认为80）建立一个TCP套接字连接
  - 通过TCP套接字，客户端向Web服务器发送一个文本的请求报文，一个请求报文由请求行、请求头部、空行和请求数据4部分组成
  - Web服务器解析请求，定位请求资源。服务器将资源复本写到TCP套接字，由客户端读取
  - 一个响应由状态行、响应头部、空行（请求空行）和响应数据（请求体）4部分组成

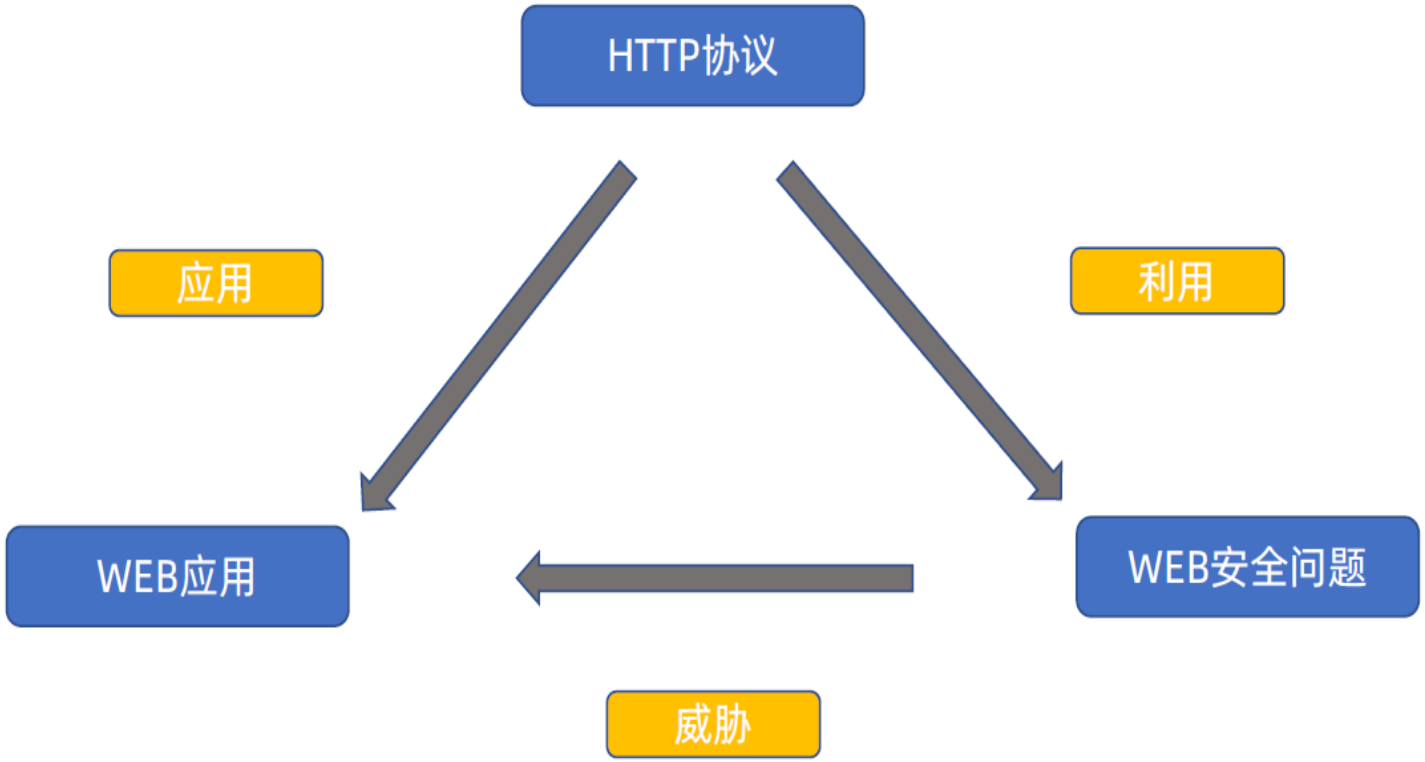
HTTP请求的构成


请求方法
请求URL
HTTP协议及版本
POST /login.html HTTP/1.1
Host:www.test.com
Connection:keep-alive
Content-Length: 70
name=ceshi&password=12345
请求头
CRLF
内容体

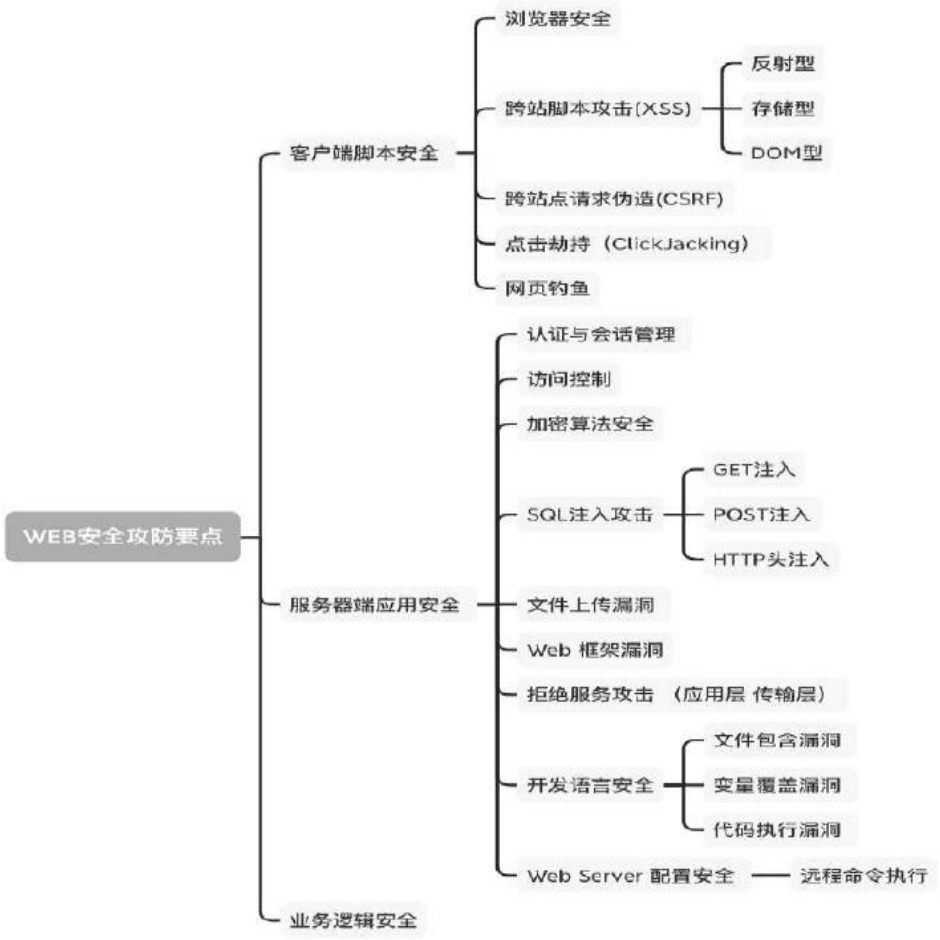
请求方法GET和POST的区别

- 从参数的传递来看,GET请求的参数是直接拼接在地址栏URL的后面,而POST请求的参数是放到请求体里面的
- 从长度限制来看,GET请求有具体的长度限制,一般不超过1024KB,而POST理论上没有,但是浏览器一般有界限
- 从安全来看,GET请求相较于POST,因为数据都是明文显示在URL上面的,所以安全和私密性不如POST

Web安全的起源



Web安全攻防分类


WEB安全攻防要点
客户端脚本安全
浏览器安全
跨站脚本攻击(XSS)
反射型
存储型
DOM型
跨站点请求伪造(CSRF)
点击劫持（ClickJacking）
网页钓鱼
服务器端应用安全
认证与会话管理
访问控制
加密算法安全
SQL注入攻击
GET注入
POST注入
HTTP头注入
文件上传漏洞
Web 框架漏洞
拒绝服务攻击 （应用层 传输层）
开发语言安全
文件包含漏洞
变量覆盖漏洞
代码执行漏洞
Web Server 配置安全
远程命令执行
业务逻辑安全

Web安全的本质

Web攻防常用工具：客户端工具

- burp suite
  - 用于攻击Web应用程序的集成平台框架
  - https://portswigger.net/burp
- curl
  - 一个功能强大灵活的网络工具，使用url的形式传输数据，支持HTTPS、FTP、Telnet等多种协议
  - https://curl.haxx.se/
- postman
  - 可视化版本的curl，是一款功能强大的网页调试与发送网页HTTP请求的工具
  - https://www.postman.com/

Web攻防常用工具：浏览器插件

- HackBar
  - Firefox浏览器插件，可以利用它快速构建一个HTTP请求，或者用它快速实现某种算法等，多用于手工测试Web漏洞
  - 打开firefox浏览器，选择附加组件，搜索hackbar，然后选择hackbar quantum进行安装
- Wappalyzer
  - 一款功能强大且非常实用的网站技术分析插件
  - https://www.wappalyzer.com/