培训教育
Training Services

CISP-PTE

Web 安全基础(0) - 介绍

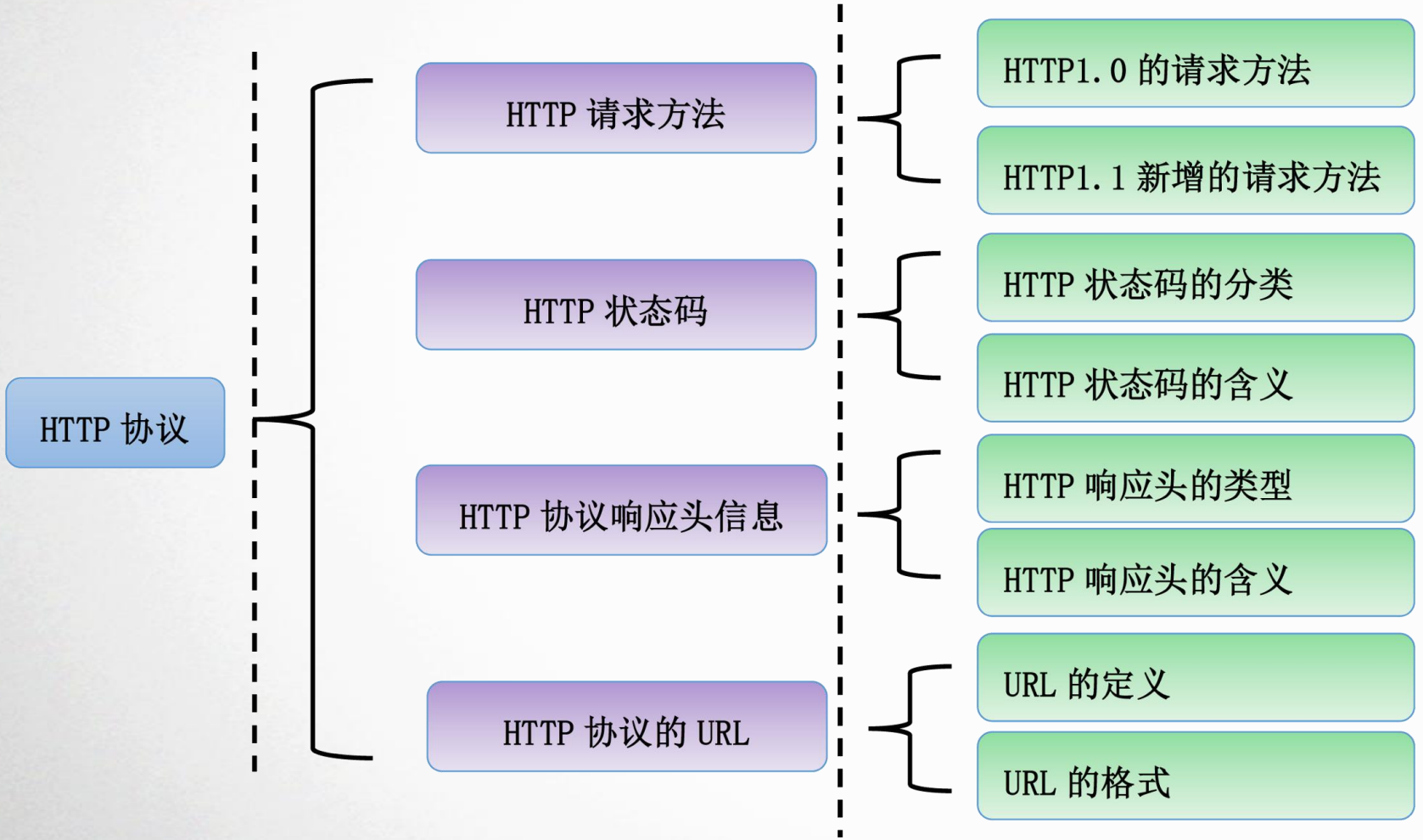
主讲：

- 通过此章我们会：
  - 了解HTTP协议的基础知识
  - 掌握HTTP协议在实际工作中的使用
  - 掌握注入漏洞相关知识以及相关的漏洞修复方法
  - 掌握XSS漏洞的多种形式和防御方法
  - 掌握请求伪造漏洞的危害和相应的检测方法
  - 掌握文件处理漏洞的分类和代码审计方法
  - 掌握访问控制漏洞的分类和漏洞防御方法
  - 掌握会话管理漏洞的特性和防护方法

知识体介绍

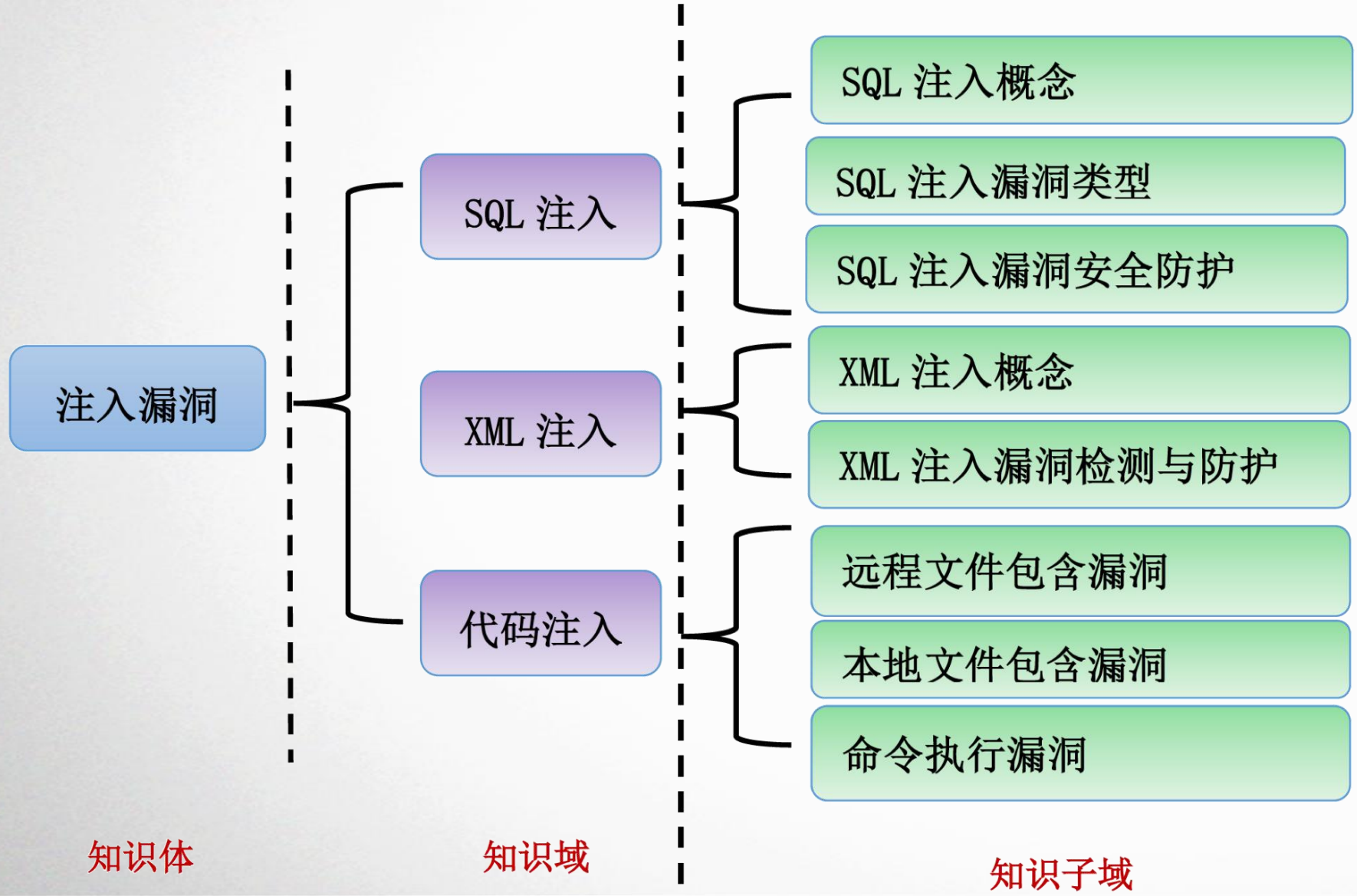
- HTTP协议
- 注入漏洞
- XSS漏洞
- 请求伪造漏洞
- 文件处理漏洞
- 访问控制漏洞
- 会话管理漏洞

HTTP协议

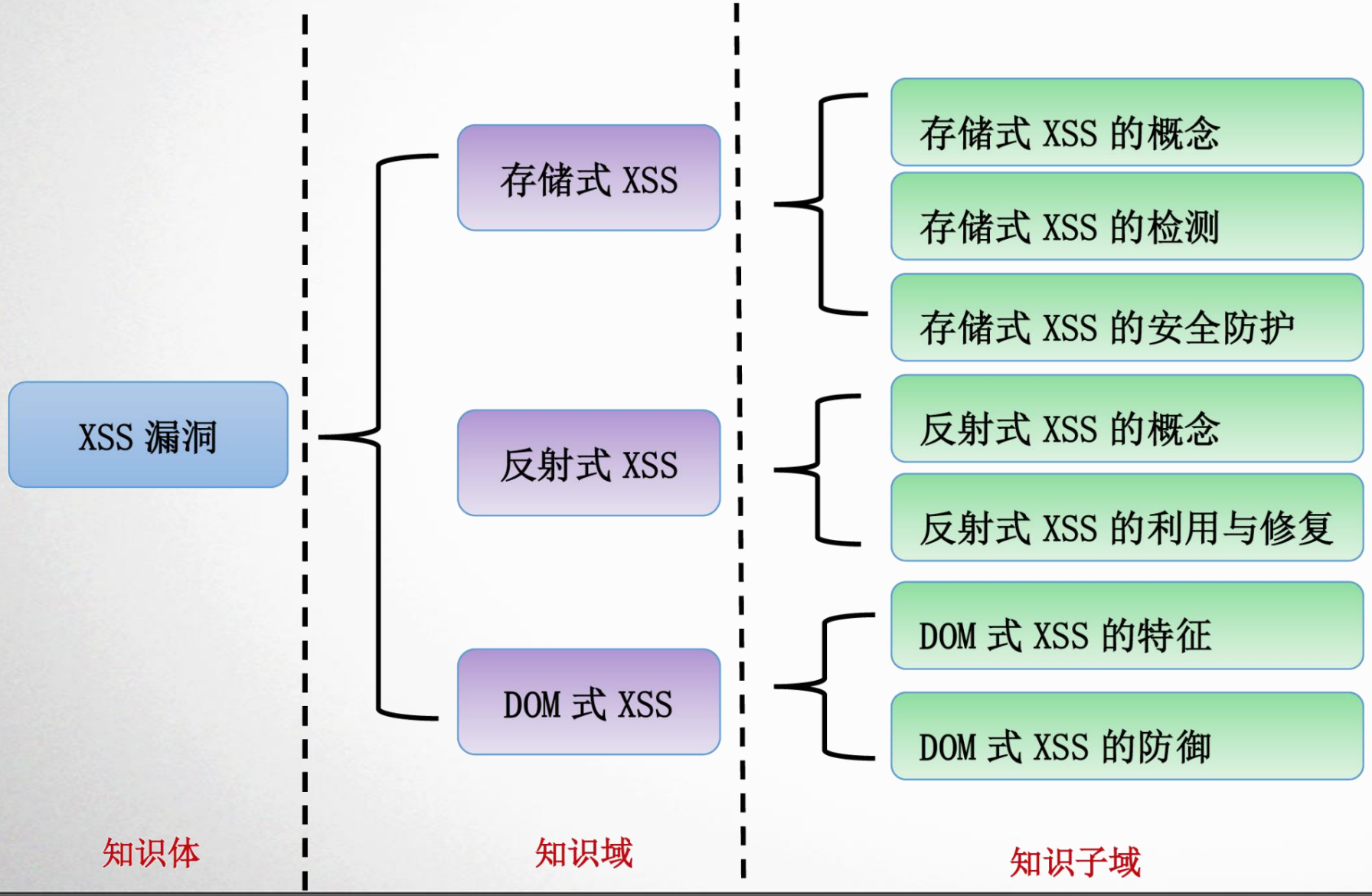


知识体　　知识域　　知识子域

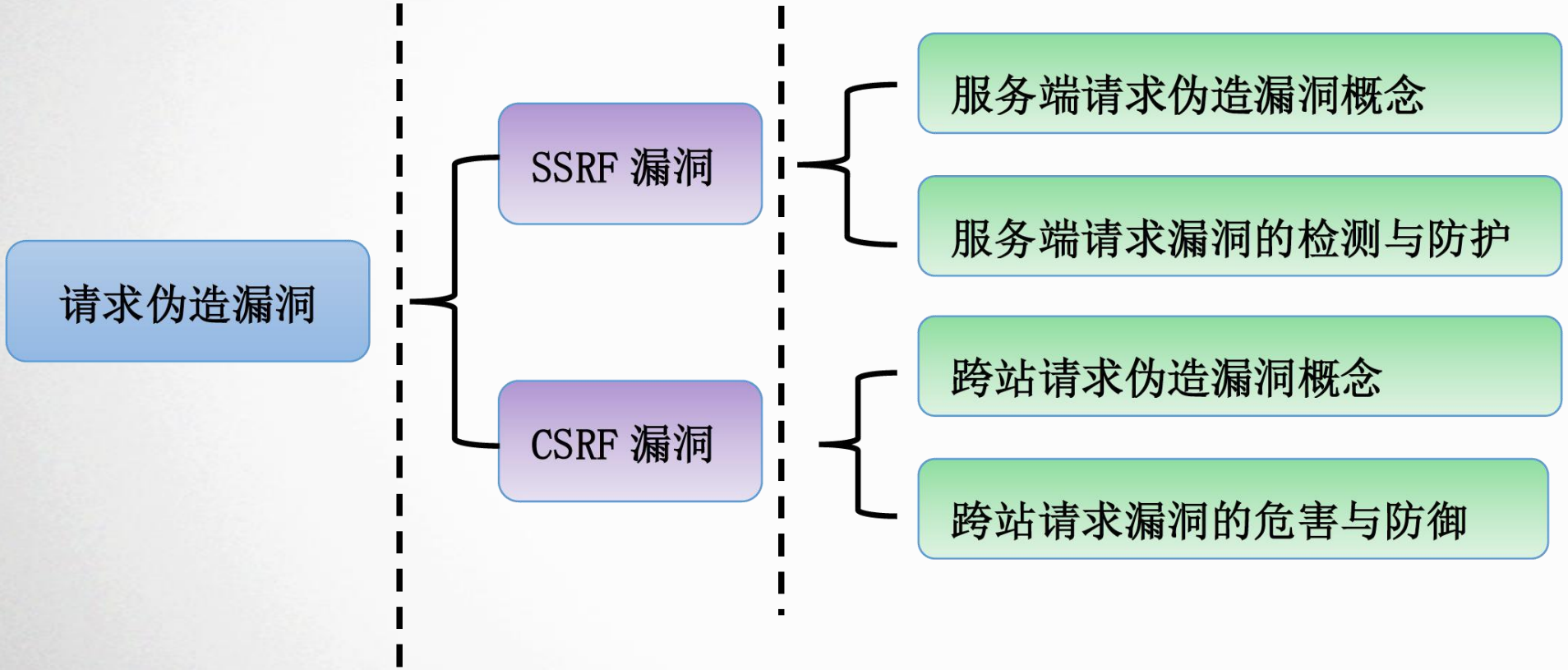
注入漏洞



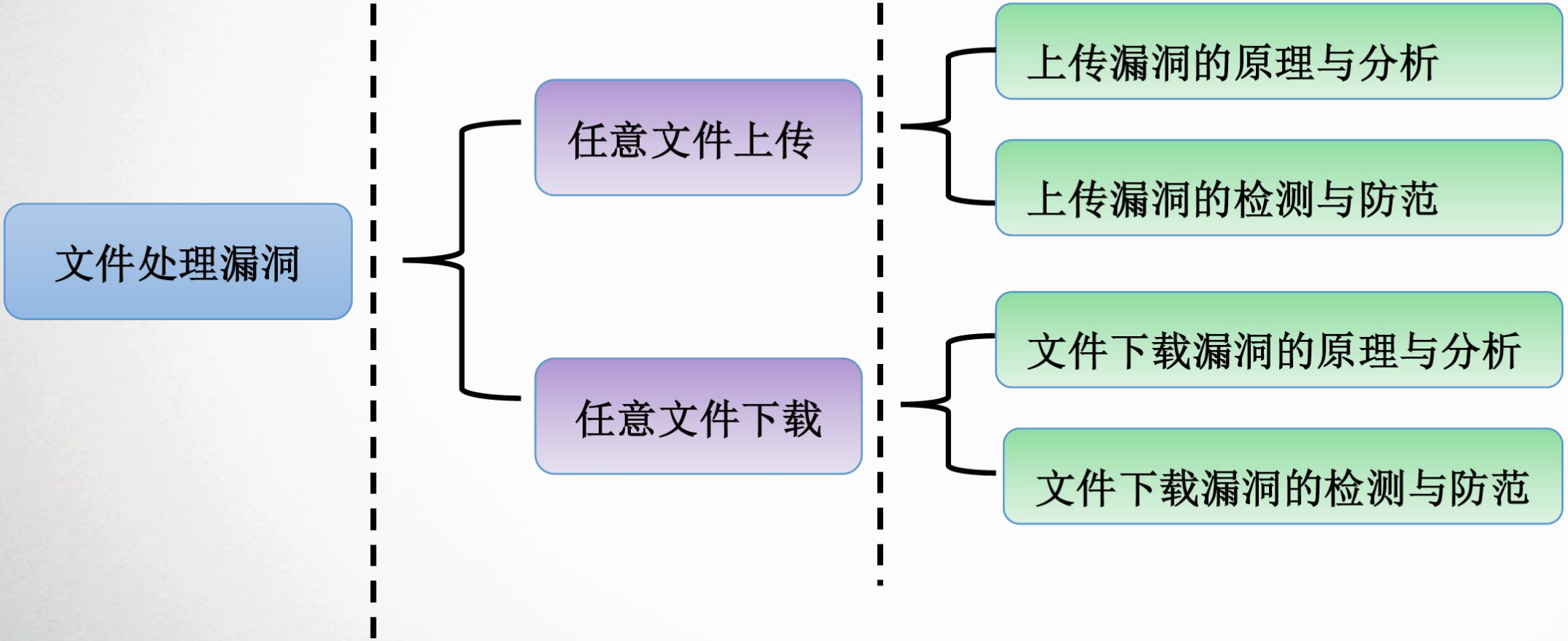
XSS漏洞



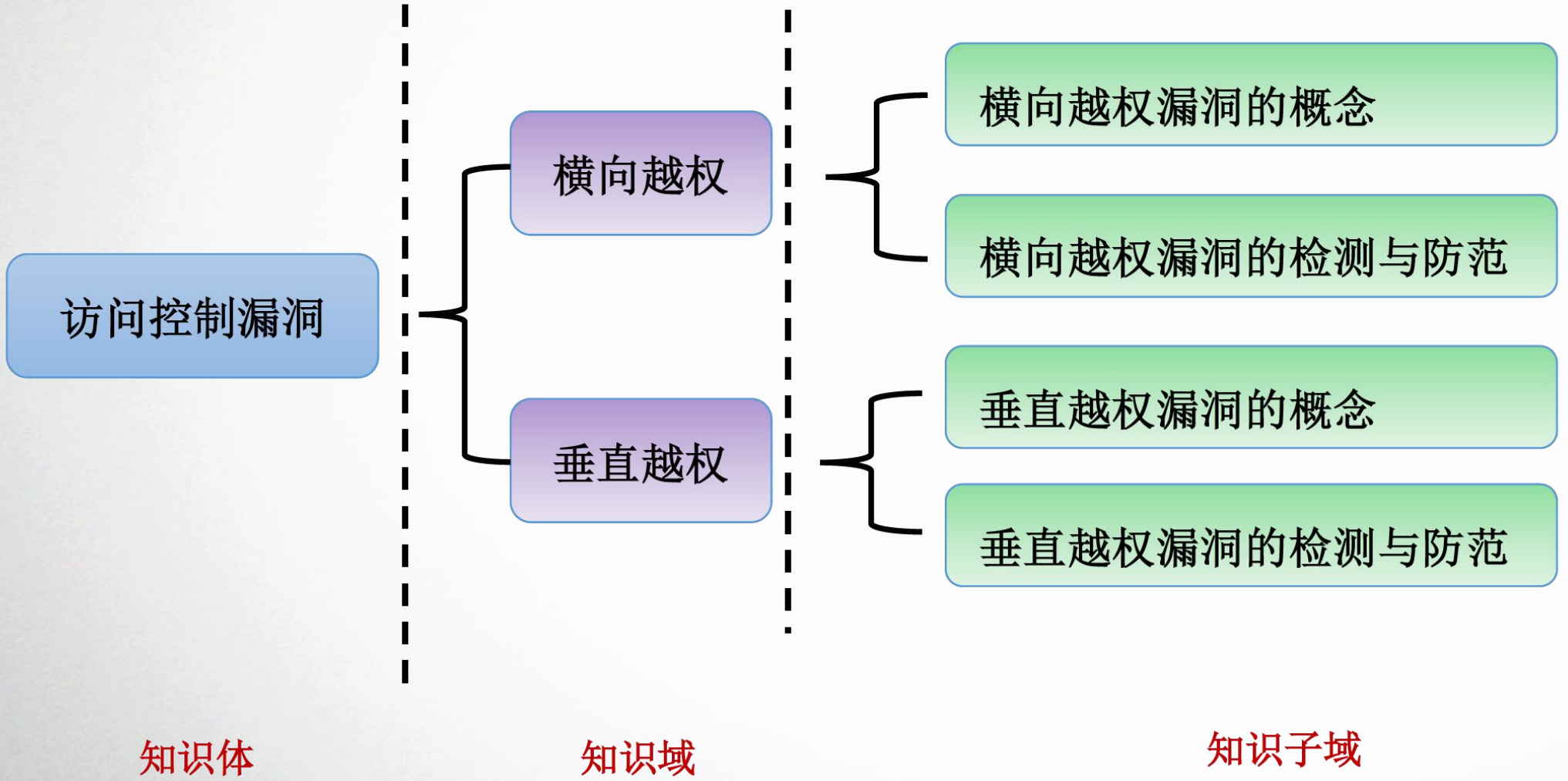
请求伪造漏洞



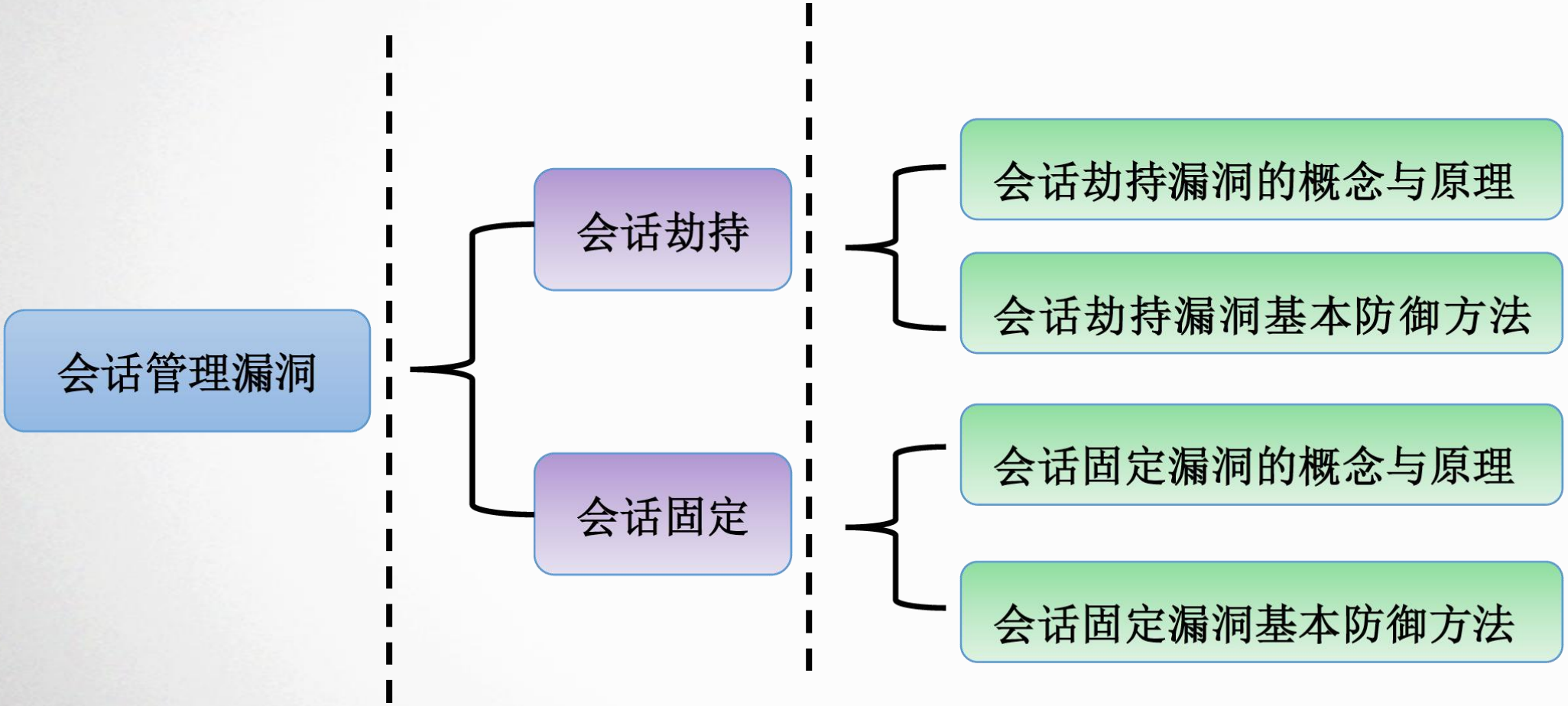
文件处理漏洞



访问控制漏洞



会话管理漏洞



用到的工具

- Burpsuite
  - 用Java做的抓包工具，可以在任意操作系统上运行
- fiddler
  - Windows下的抓包工具，相对于Burpsuite使用简单
- SQLMAP
  - sql注入工具
- DVWA
  - 搜集了各类漏洞的网站环境
- 虚拟机
  - 装有DVWA等环境的机器

基础设置

- 更改本机hosts文件
  - site1.com
  - site2.com
  - mydvwa.com
  - 上面三个地址都解析到虚拟机
  - 例如，虚拟机IP为10.0.0.1添加下面几行数据

```
10.0.0.1        site1.com
10.0.0.1        site2.com
10.0.0.1        mydvwa.com
```