注册信息安全专业人员

（渗透测试方向）知识体系大纲

发布日期：2018 年 9 月 1 日

生效日期：2018 年 9 月 1 日

中国信息安全测评中心

网神信息技术（北京）股份有限公司

目 录

第1章　前　言

网络空间信息安全作为我国信息化建设健康发展的重要因素，关系到贯彻落实科学发展观、全面建设小康社会、构建社会主义和谐社会和建设创新型社会等国家战略举措的实施，是国家安全的重要组成部分。在网络空间信息系统安全保障工作中，人，是最核心、也是最活跃的因素，人员的信息安全意识、知识与技能已经成为保障信息系统安全稳定运行的重要基本要素之一。

注册信息安全专业人员（CISP）是对我国网络基础设施和重要信息系统的信息安全专业人员进行资质评定的重要形式。多年来为落实我国有关政策“加快信息安全人才培养，增强全民信息安全意识”的指导精神，构建信息安全人才体系发挥了巨大作用。

本大纲从我国国情出发，结合我国网络基础设施和重要信息系统安全保障的实际需求，以知识体系的全面性和实用性为原则，明确规定了注册信息安全专业人员（渗透测试）应当掌握的知识要点，是 CISP-PTE/CISP-PTS 教材编制，讲师授课，学员学习，以及考试命题的重要依据。

本大纲包含以下章节：

第 2 章　渗透测试知识体系概述
第 3 章　知识类：web 安全
第 4 章　知识类：中间件安全
第 5 章　知识类：操作系统安全
第 6 章　知识类：数据库安全
第 7 章　知识类：渗透测试

第2章　注册信息安全专业人员-渗透测试知识体系概述

注册信息安全专业人员-渗透测试方向分为：

- 注册信息安全专业人员渗透测试工程师，英文为 Certified Information Security Professional - Penetration Testing Engineer ，简称 CISP-PTE。证书持有人员主要从事信息安全技术领域网站渗透测试工作，具有规划测试方案、编写项目测试计划、编写测试用例、测试报告的基本知识和能力。
- 注册信息安全专业人员渗透测试专家，英文为 Certified Information Security Professional - Penetration Testing Specialist ，简称 CISP-PTS。证书持有人员主要从事漏洞研究、代码分析工作，最新网络安全动态跟踪研究以及策划解决方案能力。

2.1 知识体系框架结构

知识体系使用组件模块化的结构，包括知识类、知识体、知识域、知识子域四个层次。

- 知识类：是对渗透测试知识领域的总体划分，包含信息安全专业人员需要掌握的四大知识类别；
- 知识体：是知识类中由属于同一技术领域的知识内容构成的相对独立、成体系的知识集合；
- 知识域：是对知识体进一步分解细化形成的完整的知识组件；
- 知识子域：是构成知识域的基本模块，由一至多个具体知识要点构成。

本大纲规定了知识子域中每一个知识要点的内容和深度要求，分为“了解”、“理解”和“掌握”三类。

- 了解：是最低深度要求，学员需要正确认识该知识要点的基本概念和原理；

- 理解：是中等深度要求，学员需要在正确认识该知识要点的基本概念和原理的基础上，深入理解其内容，并可以进一步的判断和推理；
- 掌握：是最高深度要求，学员需要正确认识该知识要点的概念、原理，并在深入理解的基础上灵活运用。

图 2-1 描述了知识体系的结构

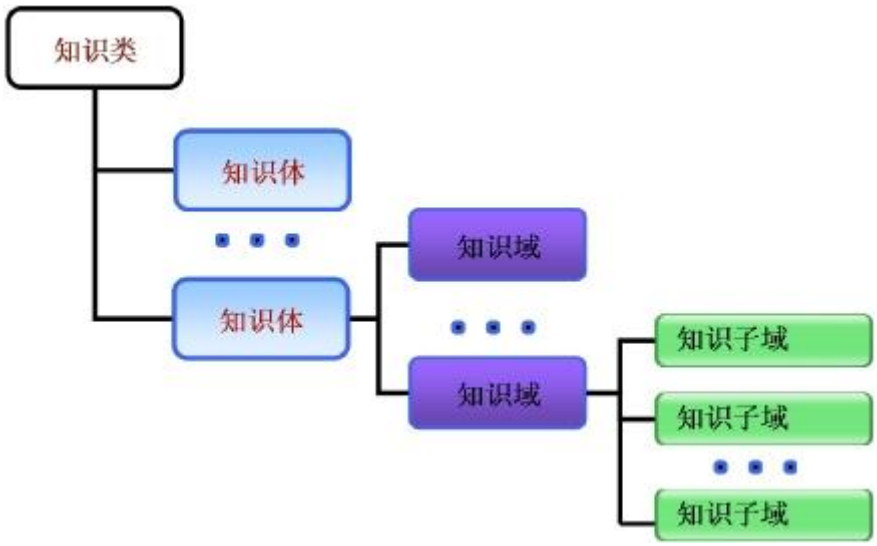

图 2-1：知识体系的组件模块结构

在整个知识体系结构中，共包括 web 安全、中间件安全、操作系统安全、数据库安全，渗透测试五个知识类，每个知识类根据其逻辑划分为多个知识体，每个知识体包含多个知识域，每个知识域由一个或多个知识子域组成。

知识体系结构共包含五个知识类，分别为：

- web 安全：主要包括 HTTP 协议、注入漏洞、XSS 漏洞、SSRF 漏洞、CSRF 漏洞、文件处理漏洞、访问控制漏洞、会话管理漏洞，代码审计等相关的技术知识和实践。
- 中间件安全：主要包括 Apache、IIS、Tomcat、weblogic、websphere、Jboss 等相关的技术知识和实践。
- 操作系统安全：主要包括 Windows 操作系统、Linux 操作系统相关技术知识和实践。

- 数据库安全：主要包括 Mssql 数据库、Mysql 数据库、Oracle 数据库、Redis 数据库相关技术知识和实践。
- 渗透测试：主要包括信息收集，漏洞发现，漏洞利用相关技术知识和实践。

图 2-2 描述了 CISP-PTE/ CISP-PTS 的知识体系结构框架：

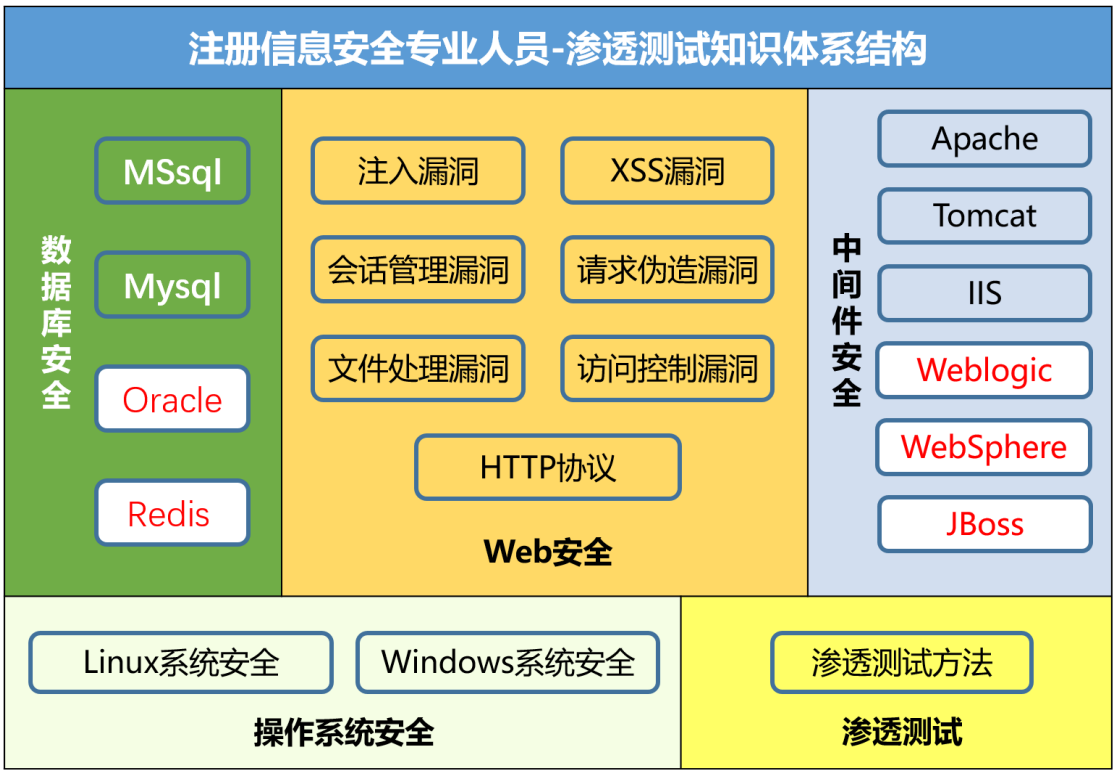

图 2-2：CISP-PTE/ CISP-PTS知识体系结构框架

（注：其中红色字体为仅在 CISP-PTS 注册培训及考试中要求掌握的知识内容。）

2.2 考试试题结构

CISP-PTE 考试题型为选择题与实操题,总分共 100 分，其中选择题 20 分，实操题 80 分，得到 70 分以上（含 70 分）为通过。

CISP-PTS 考试题型全部为实操题,总分共 100 分，得到 70 分以上（含 70 分）为通过。

证书类别 知识类别	CISP-PTE	CISP-PTS
Web 安全	50%	30%
操作系统与中间件	20%	30%
数据与日志分析	10%	10%
渗透测试	20%	30%

表 2-1：CISP-PTE/ CISP-PTS 试题结构

第3章　知识类：Web 安全

Web 安全基础是渗透测试专家需要掌握的主题知识内容之一，通过本部分的学习，学员应当：

- 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
- 掌握代码审计的方法和漏洞原理

3.1 知识体：HTTP 协议

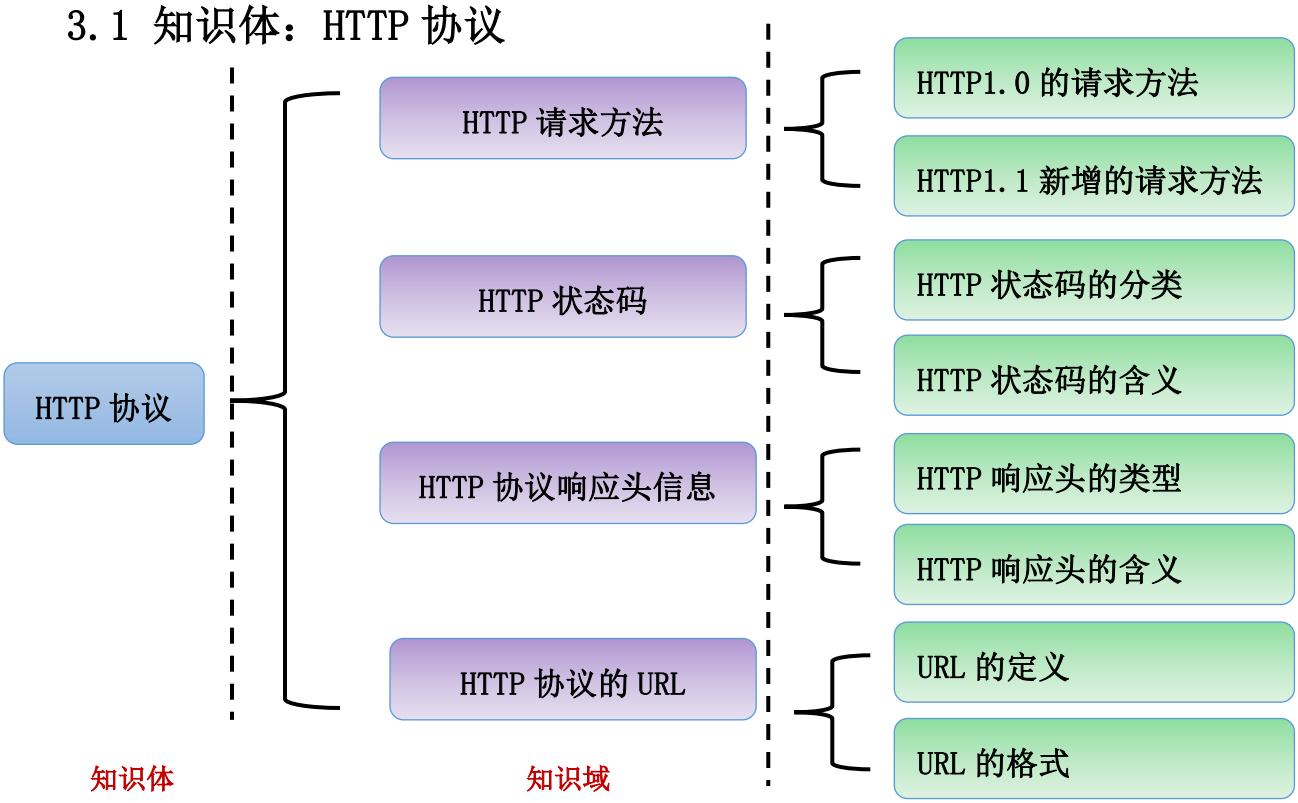

图 3-1：知识体：HTTP 协议

HTTP 协议，即超文本传输协议(Hypertext transfer protocol)。 是一种详细规定了浏览器和万维网(WWW = World Wide Web)服务器之间互相通信的规则，通过因特网传送万维网文档的数据传送协议

3.1.1 知识域：HTTP 请求方法

- 知识子域：HTTP1.0 的请求方法
  - 了解 HTTP1.0 三种请求方法，GET, POST 和 HEAD
  - 掌握 GET 请求的标准格式
  - 掌握 POST 请求提交表单，上传文件的方法
  - 了解 HEAD 请求与 GET 请求的区别
- 知识子域：HTTP1.1 新增的请求方法
  - 了解 HTTP1.1 新增了五种请求方法：OPTIONS, PUT, DELETE, TRACE 和 CONNECT 方法的基本概念
  - 掌握 HTTP1.1 新增的五种请求的基本方法和产生的请求结果

3.1.2 知识域：HTTP 的状态码

- 知识子域：HTTP 状态码的分类
  - 了解 HTTP 状态码的规范
  - 了解 HTTP 状态码的作用
  - 掌握常见的 HTTP 状态码
- 知识子域：HTTP 状态码的含义
  - 了解 HTTP 状态码 2**,3**,4**,5** 代表的含义
  - 掌握用计算机语言获取 HTTP 状态码的方法

3.1.3 知识域：HTTP 协议响应头信息

- 知识子域：HTTP 响应头的含义
  - 了解常见的 HTTP 响应头

- 掌握 HTTP 响应头的作用

- 知识子域：HTTP 响应头的类型
  - 了解 HTTP 响应头的名称
  - 掌握 HTTP 响应头的格式

3.1.4 知识域：HTTP 协议中的 URL

- 知识子域：URL 的基本构成
  - 了解 URL 的基本概念
  - 了解 URL 的结构
  - 掌握 URL 编码格式

3.2 知识体：注入漏洞

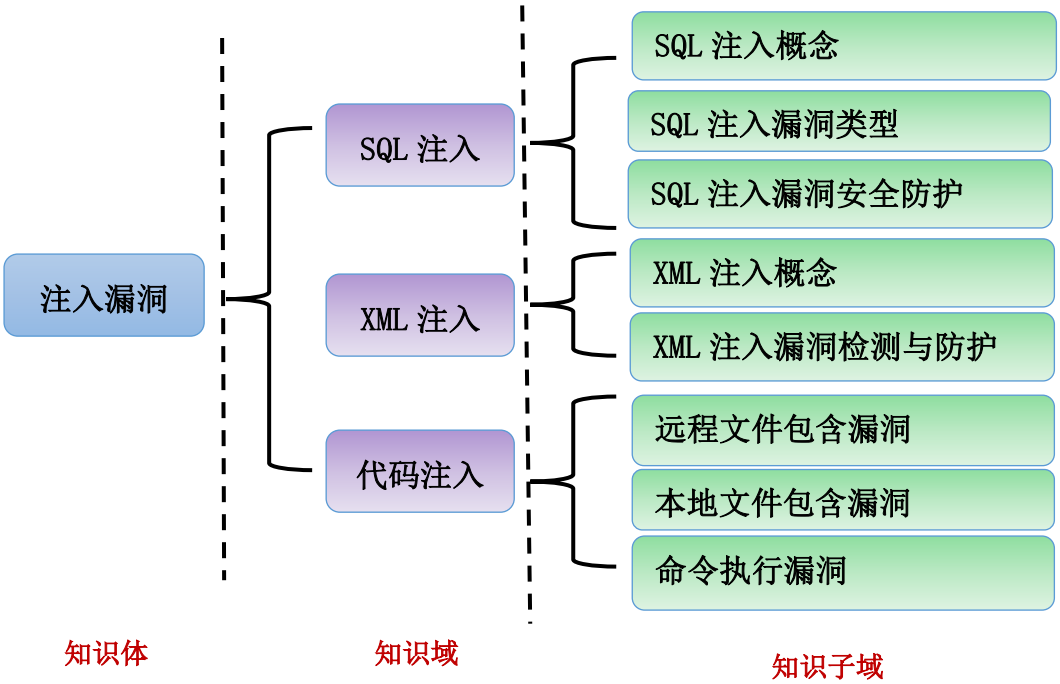

图 3-2：知识体：注入漏洞

3.2.1 知识域：SQL 注入

所谓 SQL 注入，就是通过把 SQL 命令插入到 Web 表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行指定的 SQL 语句。具体来说，它是利用现有应用程序，将 SQL 语句注入到后台数据库引擎执行的能力，它可以通过在 Web 表单中输入 SQL 语句得到一个存在安全漏洞的网站上的数据，而不是按照设计者意图去执行 SQL 语句。

- 知识子域：SQL 注入的概念
  - ◆ 了解 SQL 注入漏洞原理
  - ◆ 了解 SQL 注入漏洞对于数据安全的影响
  - ◆ 掌握 SQL 注入漏洞的方法
- 知识子域：SQL 注入的类型
  - ◆ 了解常见数据库的 SQL 查询语法
  - ◆ 掌握 MSSQL,MYSQL,ORACLE 数据库的注入方法
  - ◆ 掌握 SQL 注入漏洞的类型
- 知识子域：SQL 注入的安全防护
  - ◆ 掌握 SQL 注入漏洞修复和防范方法
  - ◆ 掌握一些 SQL 注入漏洞检测工具的使用方法

3.2.2 知识域：XML 注入

XML 外部实体注入(XML External Entity)，XML 用于标记电子文件使其具有结构性的标记语言，可以用来标记数据、定义数据类型，是一种允许用户对自己的标记语言进行定义的源语言。XML 文档结构包括 XML 声明、DTD 文档类型定义（可选）、文档元素。当允许引用外部实体时，通过构造恶意内容，可导致读取任意文件、执行系统命令、探测内网端口等危害。

- 知识子域：XML 注入概念
  - ◆ 了解什么是 XML 注入漏洞
  - ◆ 了解 XML 注入漏洞产生的原因

- 知识子域：XML 注入漏洞检测与防护
  - ◆ 掌握 XML 注入漏洞的利用方式
  - ◆ 掌握如何修复 XML 注入漏洞

3.2.3 知识域：代码注入

- 知识子域：远程文件包含漏洞(RFI)

即服务器通过 PHP 的特性（函数）去包含任意文件时，由于要包含的这个文件来源过滤不严格，从而可以去包含一个恶意文件，攻击者就可以远程构造一个特定的恶意文件达到攻击目的。

- ◆ 了解什么是远程文件包含漏洞。
- ◆ 了解远程文件包含漏洞所用到的函数。
- ◆ 掌握远程文件包含漏洞的利用方式。
- ◆ 掌握远程文件包含漏洞代码审计方法。
- ◆ 掌握修复远程文件包含漏洞的方法。

- 知识子域：本地文件包含漏洞(LFI)

文件包含漏洞的产生原因是 PHP 语言在通过引入文件时，引用的文件名，用户可控，由于传入的文件名没有经过合理的校验，或者校验被绕过，从而操作了预想之外的文件，就可能导致意外的文件泄露甚至恶意的代码注入。当被包含的文件在服务器本地时，就形成的本地文件包含漏洞。了解 PHP 脚本语言本地文件包含漏洞形成的原因，通过代码审计可以找到漏洞，并且会修复该漏洞。

- ◆ 了解什么是本地文件包含漏洞。
- ◆ 了解本地文件包含漏洞产生的原因。
- ◆ 掌握本地文件包含漏洞利用的方式。
- ◆ 了解 PHP 语言中的封装协议。
- ◆ 掌握本地文件包含漏洞修复方法。

- 知识子域：命令执行漏洞(Command Injection)

Command Injection，即命令注入攻击，是指这样一种攻击手段，黑客通过把 HTML 代码输入一个输入机制(例如缺乏有效验证限制的表格域)来改变网页的动态 生成的内容。使用系统命令是一项危险的操作，尤其在你试图使用远程数据来构造要执行的命令时更是如此。如果使用了被污染数据，命令注入漏洞就产生了。

- ◆ 了解什么是命令注入漏洞。
- ◆ 了解命令注入漏洞对系统安全产生的危害。
- ◆ 掌握脚本语言中可以执行系统命令的函数。
- ◆ 了解第三方组件存在的代码执行漏洞，如 struts2。
- ◆ 掌握命令注入漏洞的修复方法。

3.3 知识体：跨站脚本（XSS）漏洞

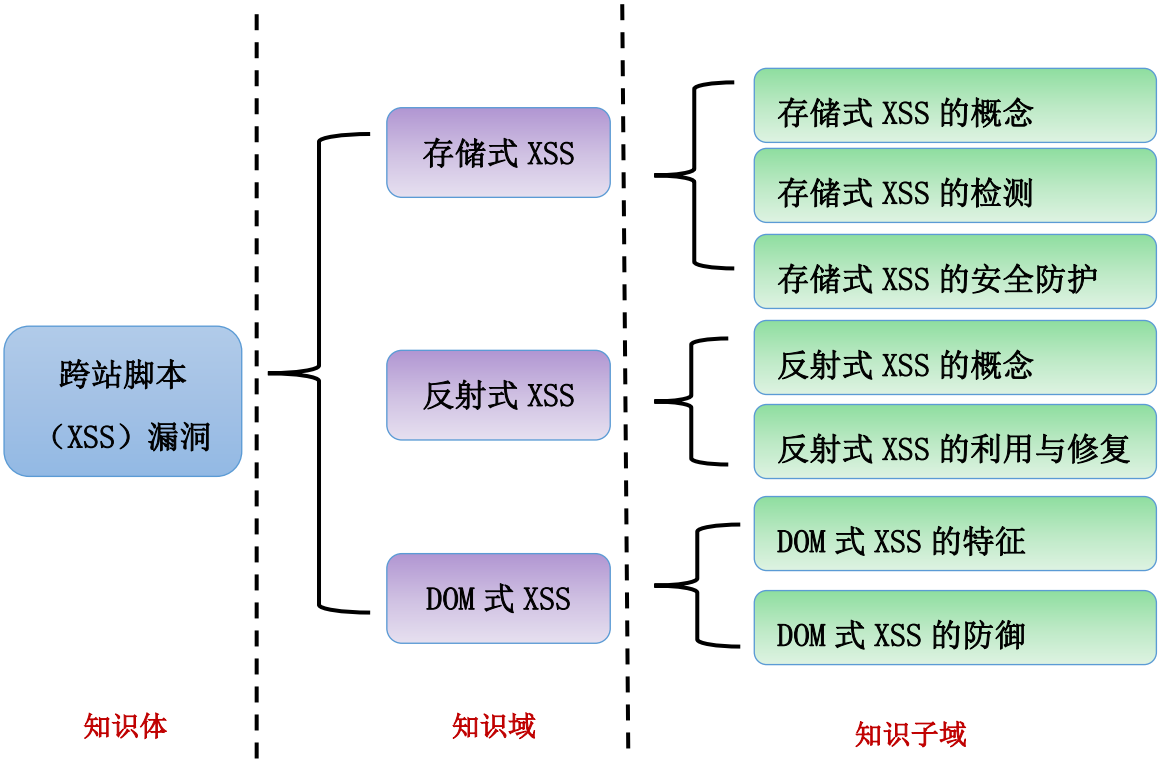

图 3-3：知识体：跨站脚本（XSS）漏洞

XSS 是一种经常出现在 web 应用中的计算机安全漏洞，它允许恶意 web 用户将代码植入到提供给其它用户使用的页面中。比如这些代码包括 HTML 代码和客户端脚本。攻击者利用 XSS 漏洞旁路掉访问控制——例如同源策略(same origin policy)。这种类型的漏洞由于被黑客用来编写危害性更大的网络钓鱼(Phishing)攻击而变得广为人知。对于跨站脚本攻击，黑客界共识是：跨站脚本攻击是新型的“缓冲区溢出攻击”，而 JavaScript 是新型的“ShellCode”。

3.3.1 知识域：存储式 XSS 漏洞

存储型 XSS，代码是存储在服务器中的，如在个人信息或发表文章等地方，加入代码，如果没有过滤或过滤不严，那么这些代码将储存到服务器中，用户访问该页面的时候触发代码执行。

- 知识子域：存储式 XSS 的概念
  - 了解什么是存储式 XSS 漏洞
  - 了解存储式 XSS 漏洞对安全的影响
- 知识子域：存储式 XSS 的检测
  - 了解存储式 XSS 漏洞的特征和检测方法
  - 掌握存储式 XSS 漏洞的危害
- 知识子域：存储式 XSS 的安全防护
  - 掌握修复存储式 XSS 漏洞的方式
  - 了解常用 WEB 漏洞扫描工具对存储式 XSS 漏洞扫描方法

3.3.2 知识域：反射式 XSS 漏洞

反射型 XSS 也被称为非持久性 XSS。当用户访问一个带有 XSS 代码的 URL 请求时，服务器端接收数据后处理，然后把带有 XSS 代码的数据发送到浏览器，浏览器解析这段带有 XSS 代码的数据后，最终造成 XSS 漏洞。这个过程就像一次反射，故称为反射型 XSS 漏洞。

- 知识子域：反射式 XSS 的概念
  - 了解什么是反射式 XSS 漏洞
  - 了解反射式 XSS 漏洞与存储式 XSS 漏洞的区别

- 知识子域：反射式 XSS 的利用与修复
  - 了解反射式 XSS 漏洞的触发形式
  - 了解反射式 XSS 漏洞利用的方式
  - 掌握反射式 XSS 漏洞检测和修复方法

3.3.3 知识域：DOM 式 XSS 漏洞

DOM 型 XSS 其实是一种特殊类型的反射型 XSS，它是基于 DOM 文档对象模型的一种漏洞。客户端的脚本程序可以通过 DOM 来动态修改页面内容，从客户端获取 DOM 中的数据并在本地执行。基于这个特性，就可以利用 JS 脚本来实现 XSS 漏洞的利用。

- 知识子域：DOM 式 XSS 的特点
  - 了解什么是 DOM 式 XSS 漏洞
  - 掌握 DOM 式 XSS 漏洞的触发形式
- 知识子域：DOM 式 XSS 的防御
  - 掌握 DOM 式 XSS 漏洞的检测方法
  - 掌握 DOM 式 XSS 漏洞的修复方法

3.4 知识体：请求伪造漏洞

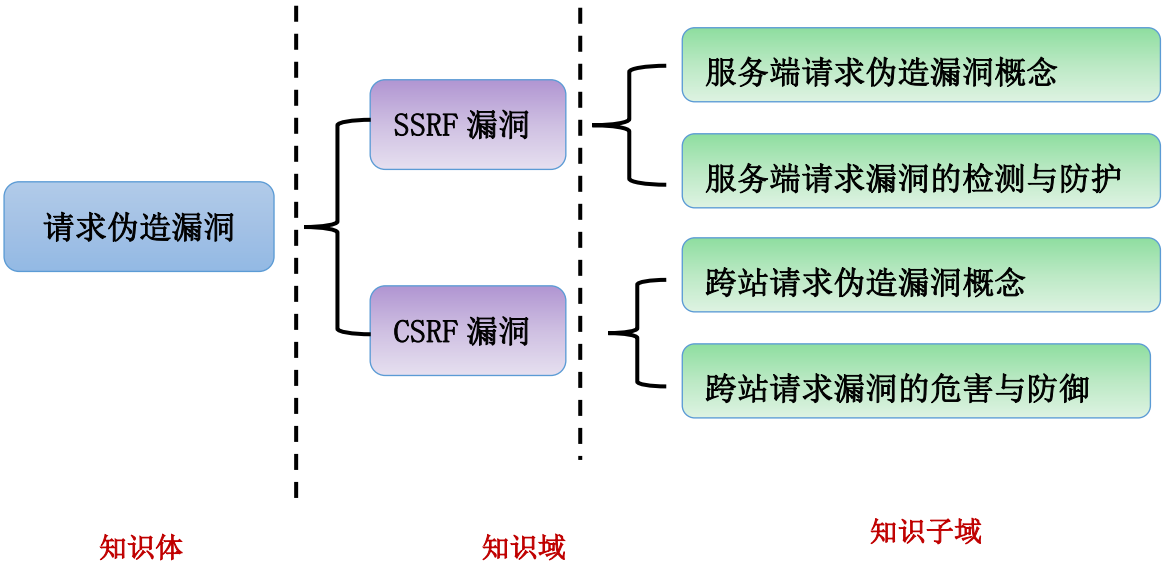

图 3-4：知识体：请求伪造漏洞

3.4.1 知识域：SSRF 漏洞

SSRF(Server-Side Request Forgery:服务器端请求伪造) 是一种由攻击者构造形成由服务端发起请求的一个安全漏洞。一般情况下，SSRF 攻击的目标是从外网无法访问的内部系统。SSRF 形成的原因大都是由于服务端提供了从其他服务器应用获取数据的功能且没有对目标地址做过滤与限制。比如从指定 URL 地址获取网页文本内容，加载指定地址的图片，下载等等。

- 知识子域：服务端请求伪造漏洞概念
    - 了解什么是 SSRF 漏洞
    - 了解利用 SSRF 漏洞进行端口探测的方法
- 知识子域：服务端请求伪造的检测与防护
    - 掌握 SSRF 漏洞的检测方法
    - 了解 SSRF 漏洞的修复方法

3.4.2 知识域：CSRF 漏洞

在跨站请求伪造（CSRF）攻击里面，攻击者通过用户的浏览器来注入额外的网络请求，来破坏一个网站会话的完整性。而浏览器的安全策略是允许当前页面发送到任何地址的请求，因此也就意味着当用户在浏览他/她无法控制的资源时，攻击者可以控制页面的内容来控制浏览器发送它精心构造的请求。

- 知识子域：跨站请求伪造漏洞的原理
    - 了解 CSRF 漏洞产生的原因
    - 理解 CSRF 漏洞的原理
- 知识子域：跨站请求伪造漏洞的危害与防御
    - 了解 CSRF 漏洞与 XSS 漏洞的区别
    - 掌握 CSRF 漏洞的挖掘和修复方

3.5 知识体：文件处理漏洞

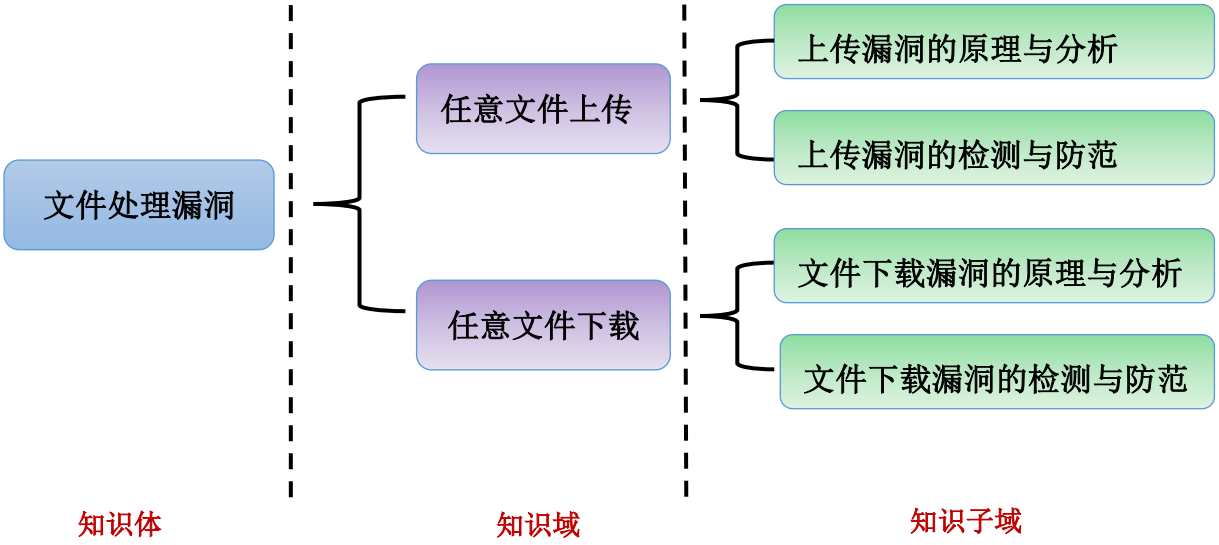

图 3-5：知识体：文件处理漏洞

3.5.1 知识域：任意文件上传

- 知识子域：上传漏洞的原理
  - ◆ 了解任意文件上传漏洞产生的原因
  - ◆ 了解服务端语言对上传文件类型限制方法
- 知识子域：上传漏洞的检测与防范
  - ◆ 了解任意文件上传漏洞的危害
  - ◆ 掌握上传漏洞的检测思路和修复方法

3.5.2 知识域：任意文件下载

- 知识子域： 文件下载漏洞的原理
  - ◆ 了解什么是文件下载漏洞
  - ◆ 掌握通过文件下载漏洞读取服务端文件的方法
- 知识子域： 任意文件下载漏洞的检测与防护
  - ◆ 掌握能够通过代码审计和测试找到文件下载漏洞

◆ 掌握修复文件下载漏洞的方法

3.6 知识体：访问控制漏洞

了解什么是访问控制漏洞，了解什么是越权，越权可以分为横向越权和垂直越权，前者指的是攻击者尝试访问与他拥有相同权限的用户的资源;而后者指的是一个低级别攻击者尝试访问高级别用户的资源。

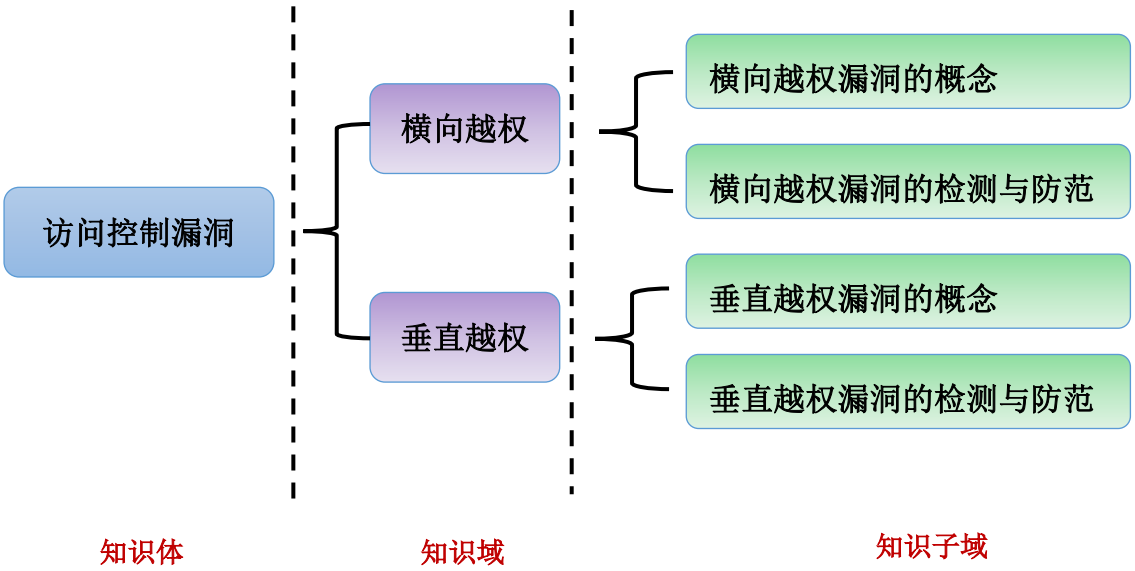

图 3-6：知识体：访问控制漏洞

3.6.1 知识域：横向越权

- 知识子域：横向越权漏洞的概念
  - ◆ 了解横向越权漏洞的基本概念
  - ◆ 了解横向越权漏洞的形式
- 知识子域：横向越权漏洞的利于与防范
  - ◆ 了解横向越权漏洞对网站安全的影响
  - ◆ 掌握横向越权漏洞的测试和修复方法

3.6.2 知识域：垂直越权

- 知识子域：垂直越权漏洞的概念
  - 了解垂直越权漏洞的基本概念
  - 了解垂直越权漏洞的种类和形式
- 知识子域：垂直越权漏洞的检测与防范
  - 了解对网站安全的影响
  - 掌握越权漏洞的测试方法和修复

3.7 知识体：会话管理漏洞

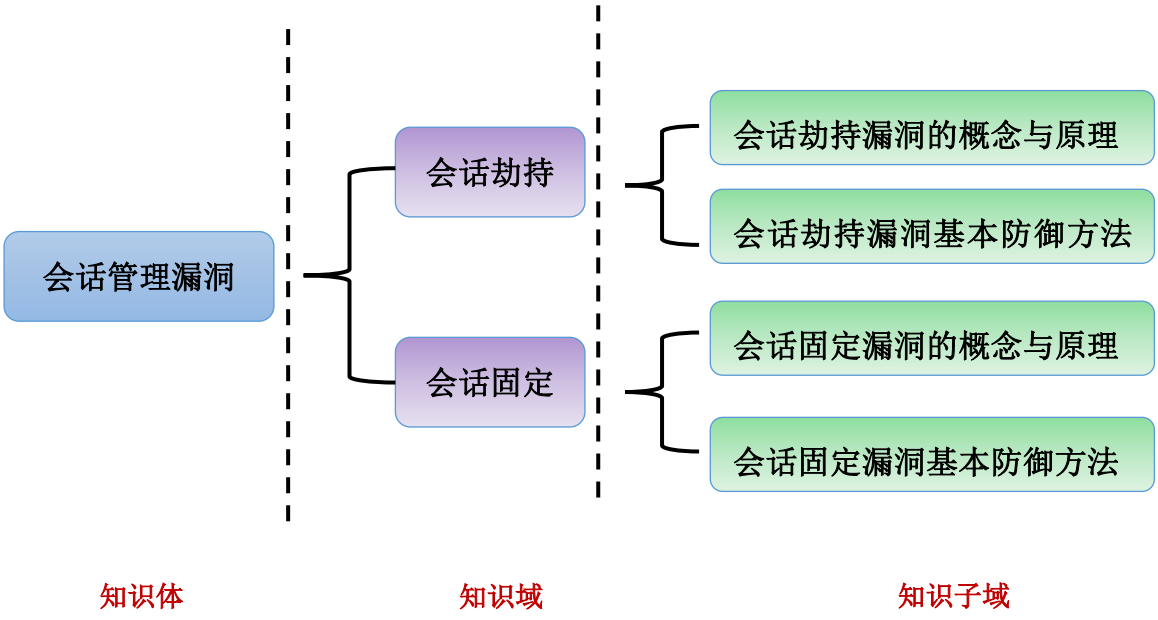

图 3-7：知识体：会话管理漏洞

会话管理漏洞可分为会话固定漏洞，会话劫持漏洞。

3.7.1 知识域：会话劫持

会话劫持（Session hijacking），这是一种通过获取用户 Session ID 后，使用该 Session ID 登录目标账号的攻击方法，此时攻击者实际上是使用了目标

账户的有效 Session。会话劫持的第一步是取得一个合法的会话标识来伪装成合法用户，因此需要保证会话标识不被泄漏。

- 知识子域：会话劫持漏的概念与原理
  - ◆ 了解什么是会话劫持漏洞
  - ◆ 了解会话劫持漏洞的危害
- 知识子域：会话劫持漏洞基本防御方法
  - ◆ 了解 Session 机制
  - ◆ 了解 HttpOnly 的设置方法
  - ◆ 掌握会话劫持漏洞防御方法

3.7.2 知识域：会话固定

会话固定（Session fixation）是一种诱骗受害者使用攻击者指定的会话标识（SessionID）的攻击手段。这是攻击者获取合法会话标识的最简单的方法。会话固定也可以看成是会话劫持的一种类型，原因是会话固定的攻击的主要目的同样是获得目标用户的合法会话，不过会话固定还可以是强迫受害者使用攻击者设定的一个有效会话，以此来获得用户的敏感信息。了解什么是会话管理漏洞，通过代码审计可以找到该漏洞并修复漏洞。

- 知识子域：会话固定漏洞的概念与原理
  - ◆ 了解什么是会话固定漏洞
  - ◆ 了解会话固定漏洞的检测方法
- 知识子域：会话固定漏洞基本防御方法
  - ◆ 了解会话固定漏洞的形成的原因
  - ◆ 了解会话固定漏洞的风险
  - ◆ 掌握会话固定漏洞的防范方法

第4章　知识类：中间件安全

中间件安全基础是注册信息安全专业人员需要掌握的通用基础知识。通过本部分的学习，学员应当：

- 了解中间件的基本概念和加固方法
- 掌握主流中间件的权限配置，解析漏洞风险
- 掌握 JAVA 开发的中间件反序列化漏洞风险

4.1 知识体：主流的中间件

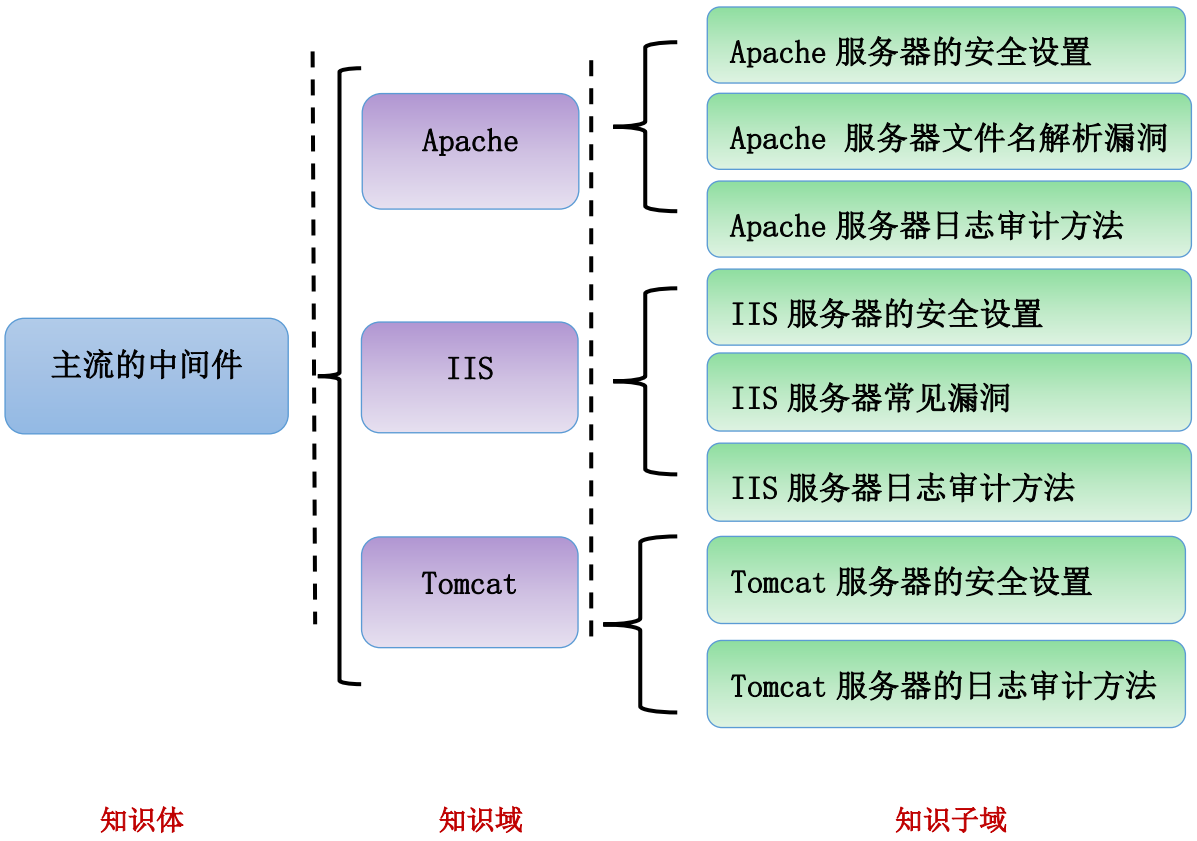

图 4-1：知识体：主流的中间件

4.1.1 知识域：Apache

Apache 是世界使用排名第一的 Web 服务器软件，它可以运行在几乎所有广泛使用的计算机平台上，由于其跨平台和安全性被广泛使用，是最流行的 Web 服务器端软件之一。Apache 自身的安全性是很高的，但是人为的错误设置会导致 Apache 产生安全问题。

- 知识子域：Apache 服务器的安全设置
  - ◆ 了解当前 Apache 服务器的运行权限
  - ◆ 了解控制配置文件和日志文件的权限，防止未授权访问
  - ◆ 了解设置日志记录文件、记录内容、记录格式
  - ◆ 了解禁止 Apache 服务器列表显示文件的方法
  - ◆ 了解修改 Apache 服务器错误页面重定向的方法
  - ◆ 掌握设置 Web 目录的读写权限，脚本执行权限的方法
- 知识子域：Apache 服务器文件名解析漏洞
  - ◆ 了解 Apache 服务器解析漏洞的利用方式
  - ◆ 掌握 Apache 服务器文件名解析漏洞的防御措施
- 知识子域：Apache 服务器日志审计
  - ◆ 掌握 Apache 服务器日志审计方法

4.1.2 知识域：IIS

IIS 全称为 Internet Information Service（Internet 信息服务），它的功能是提供信息服务，如架设 http、ftp 服务器等

- 知识子域：IIS 服务器的安全设置
  - ◆ 了解身份验证功能，能够对访问用户进行控制
  - ◆ 了解利用账号控制 web 目录的访问权限，防止跨目录访问
  - ◆ 了解为每个站点设置单独的应用程序池和单独的用户的方法
  - ◆ 了解取消上传目录的可执行脚本的权限的方法
  - ◆ 启用或禁用日志记录，配置日志的记录选项

- 知识子域：IIS 服务器的常见漏洞
    - ◆ 掌握 IIS6，IIS7 的文件名解析漏洞
    - ◆ 掌握 IIS6 写权限的利用
    - ◆ 掌握 IIS6 存在的短文件名漏洞
- 知识子域：IIS 服务器日志审计方法
    - ◆ 掌握 IIS 日志的审计方法

4.1.3 知识域：Tomcat

Tomcat 是一个小型的轻量级应用服务器，在中小型系统和并发访问用户不是很多的场合下被普遍使用，是开发和调试 JSP 程序的首选。

- 知识子域：Tomcat 服务器的安全设置
    - ◆ 了解 Tomcat 服务器启动的权限
    - ◆ 了解 Tomcat 服务器后台管理地址和修改管理账号密码的方法
    - ◆ 了解隐藏 Tomcat 版本信息的方法
    - ◆ 了解如何关闭不必要的接口和功能
    - ◆ 了解如何禁止目录列表，防止文件名泄露
    - ◆ 掌握 Tomcat 服务器通过后台获取权限的方法
    - ◆ 掌握 Tomcat 样例目录 session 操纵漏洞
- 知识子域：Tomcat 服务器的日志审计方法
    - ◆ 了解 Tomcat 的日志种类
    - ◆ 掌握 Tomcat 日志的审计方法

4.2 知识体：JAVA 开发的中间件

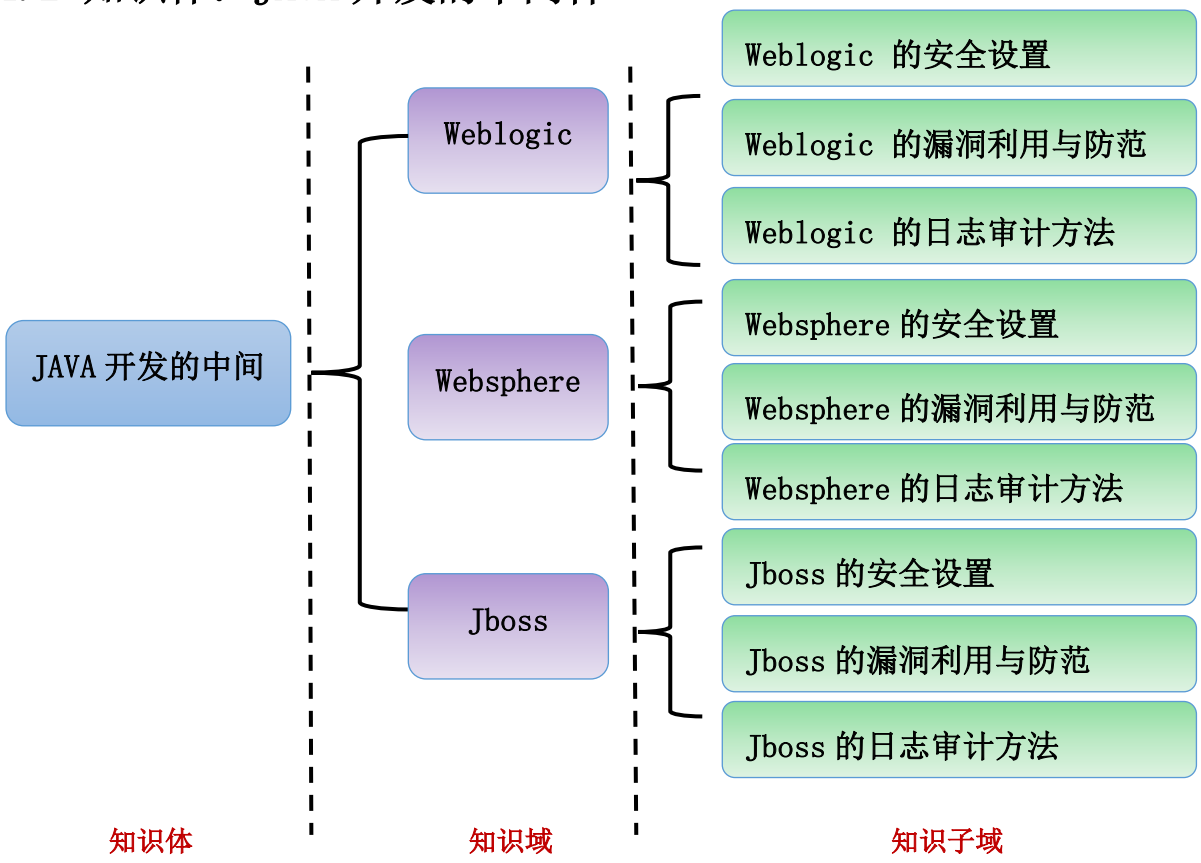

图 4-2：知识体：JAVA 开发的中间件

4.2.1 知识域：Weblogic

WebLogic 是美国 Oracle 公司出品的一个 application server，确切的说是一个基于 JAVAEE 架构的中间件，WebLogic 是用于开发、集成、部署和管理大型分布式 Web 应用、网络应用和数据库应用的 Java 应用服务器。将 Java 的动态功能和 Java Enterprise 标准的安全性引入大型网络应用的开发、集成、部署和管理之中。

- 知识子域：Weblogic 的安全设置
  - ◆ 了解 Weblogic 的启动权限
  - ◆ 了解修改 Weblogic 的默认开放端口的方法

- ◆ 了解禁止 Weblogic 列表显示文件的方法

- 知识子域：Weblogic 的漏洞利用与防范
  - ◆ 掌握 Weblogic 后台获取权限的方法
  - ◆ 掌握 Weblogic 存在的 SSRF 漏洞
  - ◆ 掌握反序列化漏洞对 Weblogic 的影响
- 知识子域：Weblogic 的日志审计方法
  - ◆ 掌握 Weblogic 日志的审计方法

4.2.2 知识域：Websphere

Websphere 是 IBM 的软件平台。它包含了编写、运行和监视全天候的工业强度的随需应变 Web 应用程序和跨平台、跨产品解决方案所需要的整个中间件基础设施，如服务器、服务和工具。Websphere 提供了可靠、灵活和健壮的软件。

- 知识子域：Websphere 的安全设置
  - ◆ 了解 Websphere 管理的使用
  - ◆ 了解 Websphere 的安全配置
- 知识子域：Websphere 的漏洞利用与防范
  - ◆ 掌握反序列化漏洞对 Websphere 的影响
  - ◆ 掌握 Websphere 后台获取权限的方法
- 知识子域：漏洞利用与防范
  - ◆ 掌握 Websphere 的日志审计

4.2.3 知识域：Jboss

是一个基于 J2EE 的开放源代码的应用服务器。 JBoss 代码遵循 LGPL 许可，可以在任何商业应用中免费使用，而不用支付费用。JBoss 是一个管理 EJB 的容器和服务器，支持 EJB 1.1、EJB 2.0 和 EJB3 的规范。但 JBoss 核心服务不包括支持 servlet/JSP 的 WEB 容器，一般与 Tomcat 或 Jetty 绑定使用。

- 知识子域:Jboss 的安全设置

- ◆ 了解设置 jmx-console/web-console 密码的方法
- ◆ 了解开启日志功能的方法
- ◆ 了解设置通讯协议，开启 HTTPS 访问
- ◆ 了解修改 Web 的访问端口

- 知识子域：Jboss 的漏洞利用与防范
  - ◆ 掌握反序列化漏洞对 Jboss 的影响
  - ◆ JMXInvokerServlet/jmx-console/web-console 漏洞利用与防范

- 知识子域：Jboss 的日志审计方法
  - ◆ 掌握 Jboss 日志审计的方法

第5章　知识类：操作系统安全

操作系统安全基础是注册信息安全专业人员需要掌握的通用基础知识。通过本部分的学习，学员应当：

- 了解操作系统的安全基础知识
- 掌握 Windows 操作系统的账户，文件系统以及日志的安全基础知识
- 了解 Windows 系统漏洞以及第三方应用漏洞的检测和防范方法
- 掌握 Linux 操作系统的账户，文件系统以及日志的安全基础知识
- 了解 Linux 系统漏洞以及防御措施

5.1 知识体：Windows 操作系统

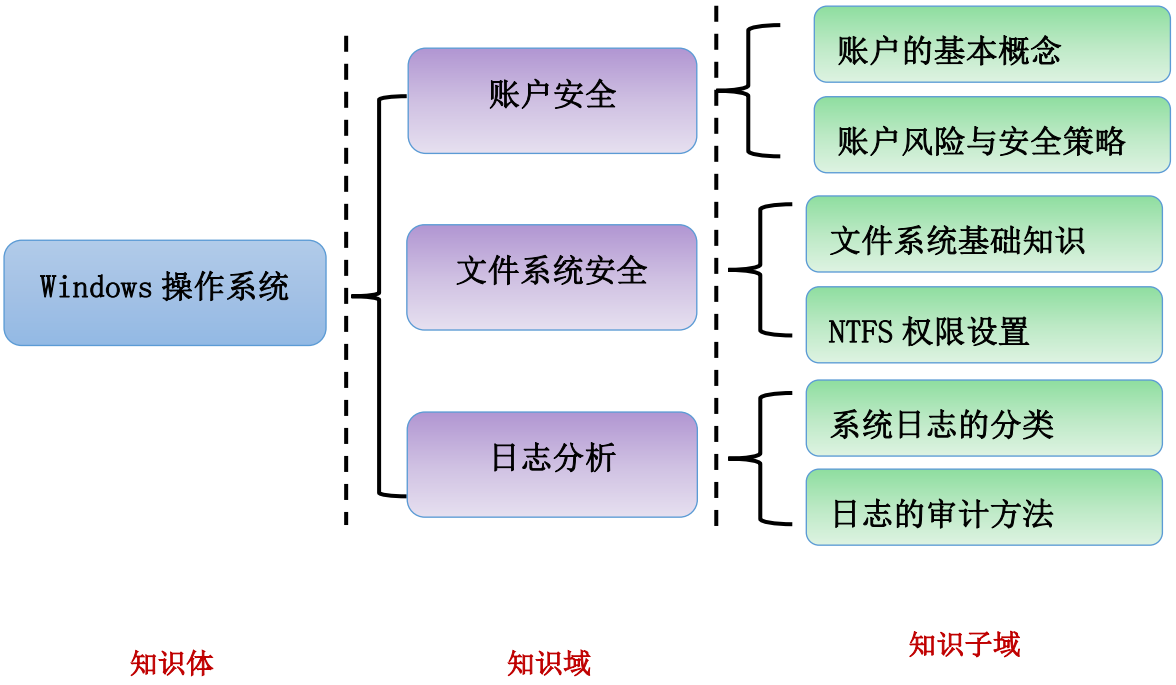

图 5-1：知识体：Windows 操作系统

5.1.1 知识域：账户安全

- 知识子域：账户的基本概念
  - ◆ Windows 用户账户和组账户权限的分配
- 知识子域：账户风险与安全策略

- ◆ 了解 Windows 用户空口令风险
- ◆ 了解多用户同时使用的安全配置
- ◆ 了解对用户登入事件进行审核方法
- ◆ 了解对远程登入账号的检查

5.1.2 知识域：文件系统安全

对于 NTFS 磁盘分区上的每一个文件和文件夹，NTFS 都存储一个远程访问控制列表（ACL，Access Control Lists），ACL 中包含有那些被授权访问该文件或者文件夹的所有用户账号、组和计算机，还包含他们被授予的访问类型。

- 知识子域：文件系统基础知识
  - ◆ 掌握 NTFS 文件权限种类
- 知识子域：NTFS 权限设置
  - ◆ 掌握通过 ACL 控制列表，设置目录或者文件的用户访问权限
  - ◆ 掌握命令行下修改目录或者文件的访问权限的方法

5.1.3 知识域：日志分析

- 知识子域：系统日志的分类
  - ◆ 了解 Windows 系统日志的种类
  - ◆ 了解 Windows 安全日志的登入类型
- 知识子域：日志的审计方法
  - ◆ 掌握日志审计的方法

5.2 知识体：Linux 操作系统

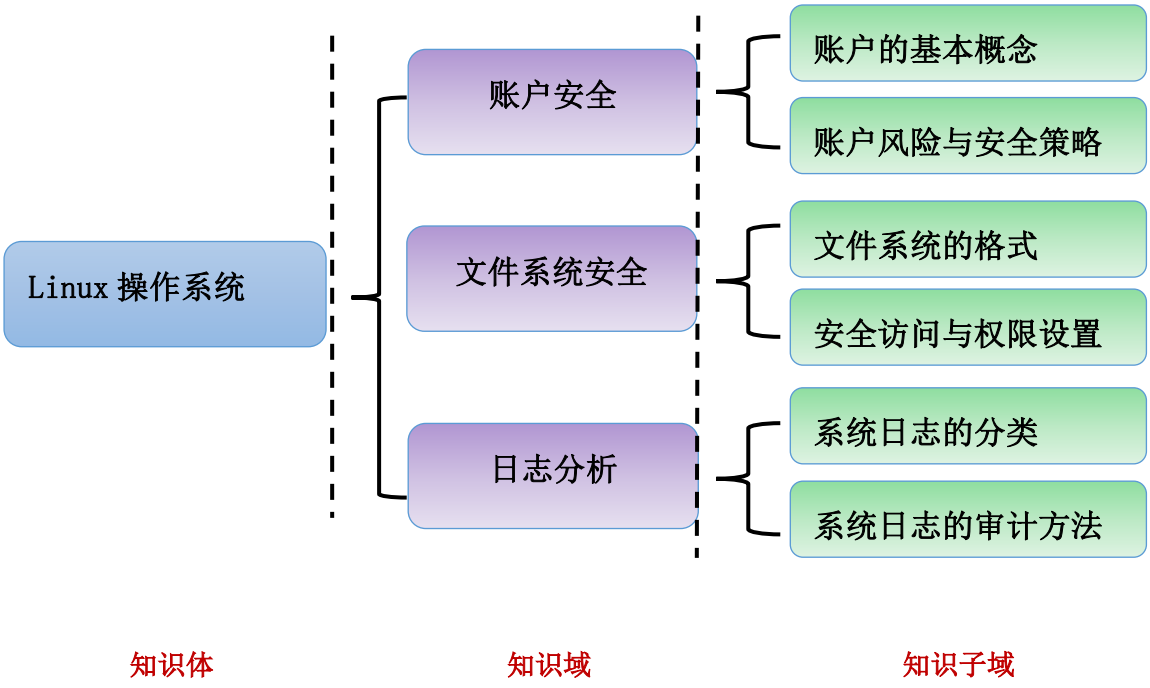

图 5-2：知识体：Linux 操作系统

5.2.1 知识域：账户安全

在 Linux 系统中，提供了多种机制来确保用户账号的正确，安全使用。合理地规划用户账号，并合理地分配权限，是保证 Linux 系统安全的第一步。

- 知识子域：账户的基本概念
  - 了解 Linux 系统中的账号和组
- 知识子域：账户风险与安全策略
  - 了解弱口令密码带来的风险
  - 掌握检查空口令的方法
  - 掌握检查系统中是否存在其它 id 为 0 的用户的方法

5.2.2 知识域：文件系统安全

Linux 系统中的每个文件和目录都有访问许可权限，通过其确定谁可以通过何种方式对文件和目录进行访问和操作检查重要目录和文件的权限

- 知识子域：文件系统的格式
    - ◆ 了解 Linux 文件系统的文件格式分类
- 知识子域：安全访问与权限设置
    - ◆ 掌握如何检查系统中存在的 SUID 和 SGID 程序
    - ◆ 掌握检查系统中任何人都有写权限的目录的方法
    - ◆ 掌握修改目录和文件权限的方法
    - ◆ 掌握搜索文件内容的方法

5.2.3 知识域：日志分析

日志对于系统安全非常重要，记录了操作系统每天发生情况，我们可以通过日志来检查错误发生的原因，或者受到攻击时攻击者留下的痕迹。日志主要的功能有：审计和监测。他还可以实时的监测系统状态，监测和追踪侵入者等等。

- 知识子域：系统日志分类
    - ◆ 了解 Linux 系统的日志种类
    - ◆ 了解 Linux 日志文件
- 知识子域：系统日志的审计方法
    - ◆ 掌握使用常用的日志查看命令，进行日志审计的方法

第6章　知识类：数据库安全

数据库安全基础是注册信息安全专业人员需要掌握的主体知识内容之一。通过本部分的学习，学员应当：

- 关系型数据与非关系型数据库的区别
- 掌握主流关系型数据库 Mssql,Mysql,Oracle 数据库角色与权限的分配
- 掌握关系型数据库的存储过程和内置函数的对安全的影响

6.1 知识体：关系型数据库

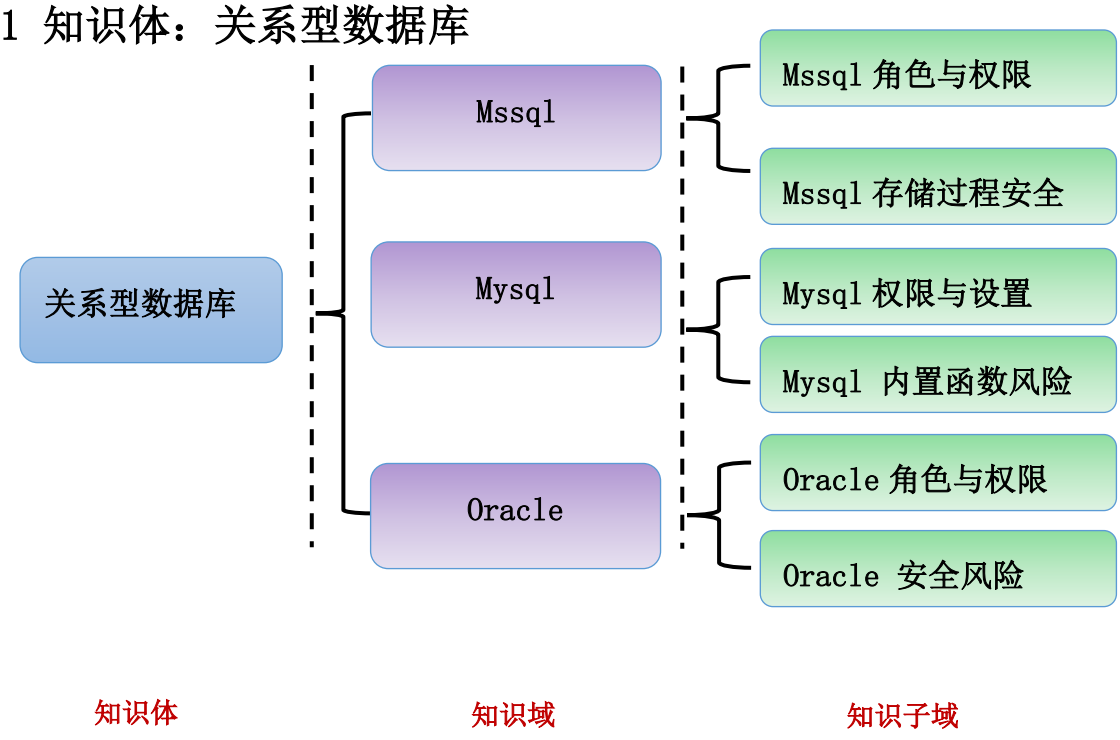

图 6-1：知识体：关系型数据库

6.1.1 知识域：Mssql 数据库

MSSQL 是指微软的 SQLServer 数据库服务器，它是一个数据库平台，提供数据库的从服务器到终端的完整的解决方案，其中数据库服务器部分，是一个数据库管理系统，用于建立、使用和维护数据库。

- 知识子域：Mssql 角色与权限
    - ◆ 了解 Mssql 数据库在操作系统中启动的权限
    - ◆ 掌握 Mssql 数据库中服务器角色和数据库角色
    - ◆ 掌握 Mssql 存在 SA 弱口令和空口令带来的危害
- 知识子域：Mssql 存储过程安全
    - ◆ 掌握 Mssql 数据库执行系统命令或者操作系统文件的存储过程
    - ◆ 掌握 Mssql 提升权限的方法

6.1.2 知识域：Mysql 数据库

MySQL 是一个真正的多用户、多线程 SQL 数据库服务器，它是一个客户机/服务器结构的实现。MySQL 是现在流行的关系数据库中其中的一种，相比其它的数据库管理系统（DBMS）来说，MySQL 具有小巧、功能齐全、查询迅捷等优点。

- 知识子域：Mysql 权限与设置
    - ◆ 了解 Mysql 在操作系统中运行的权限
    - ◆ 了解 Mysql 账户的安全策略
    - ◆ 了解 Mysql 远程访问的控制方法
    - ◆ 了解 Mysql 数据库所在目录的权限控制
- 知识子域：Mysql 内置函数风险
    - ◆ 掌握 Mysql 数据库常用函数
    - ◆ 掌握 Mysql 数据库权限提升的方法

6.1.3 知识域：Oracle 数据库

Oracle 是以高级结构化查询语言(SQL)为基础的大型关系数据库，通俗地讲它是用方便逻辑管理的语言操纵大量有规律数据的集合。是目前最流行的客户/服务器(CLIENT/SERVER)体系结构的数据库之一。

- 知识子域：Oracle 角色与权限
  - ◆ 了解 Oracle 数据库的账号管理与授权
  - ◆ 了解为不同管理员分配不同的账号的方法
  - ◆ 了解设置管理 public 角色的程序包执行权限
- 知识子域：Oracle 安全风险
  - ◆ 了解限制库文件的访问权限
  - ◆ 掌握 Oracle 执行系统命令的方法

6.2 知识体：非关系型数据库

数据库安全基础是注册信息安全专业人员需要掌握的主体知识内容之一。通过本部分的学习，学员应当：

- 了解非关系型数据库的基本概念
- 掌握 Redis 数据库存在的风险与安全加固方

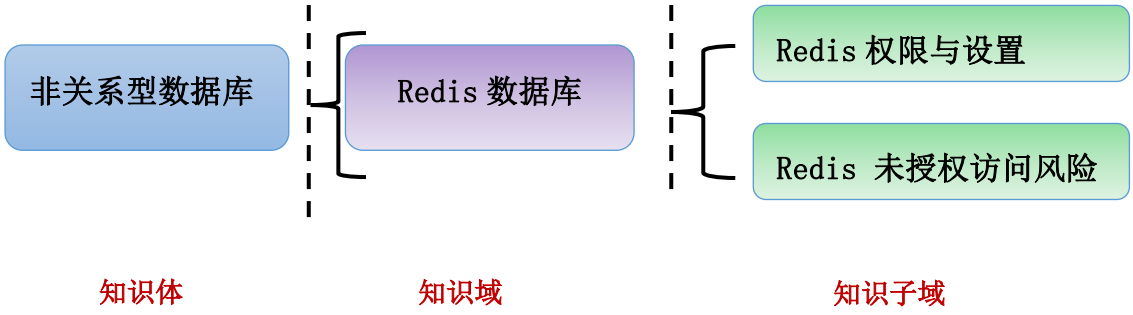

图 6-2：知识体：非关系型数据库

6.2.1 知识域：Redis 数据库

Redis 是一个开源的使用 ANSI C 语言编写、支持网络、可基于内存亦可持久化的日志型、Key-Value 数据库，并提供多种语言的 API。

- 知识子域：Redis 权限与设置
    - ◆ 了解 Redis 数据库运行权限
    - ◆ 了解 Redis 数据库的默认端口
- 知识子域：Redis 未授权访问风险
    - ◆ 掌握 Redis 未授权访问的危害
    - ◆ 掌握 Redis 开启授权的方法

第7章　知识类：　渗透测试

7.1 知识体：渗透测试方法

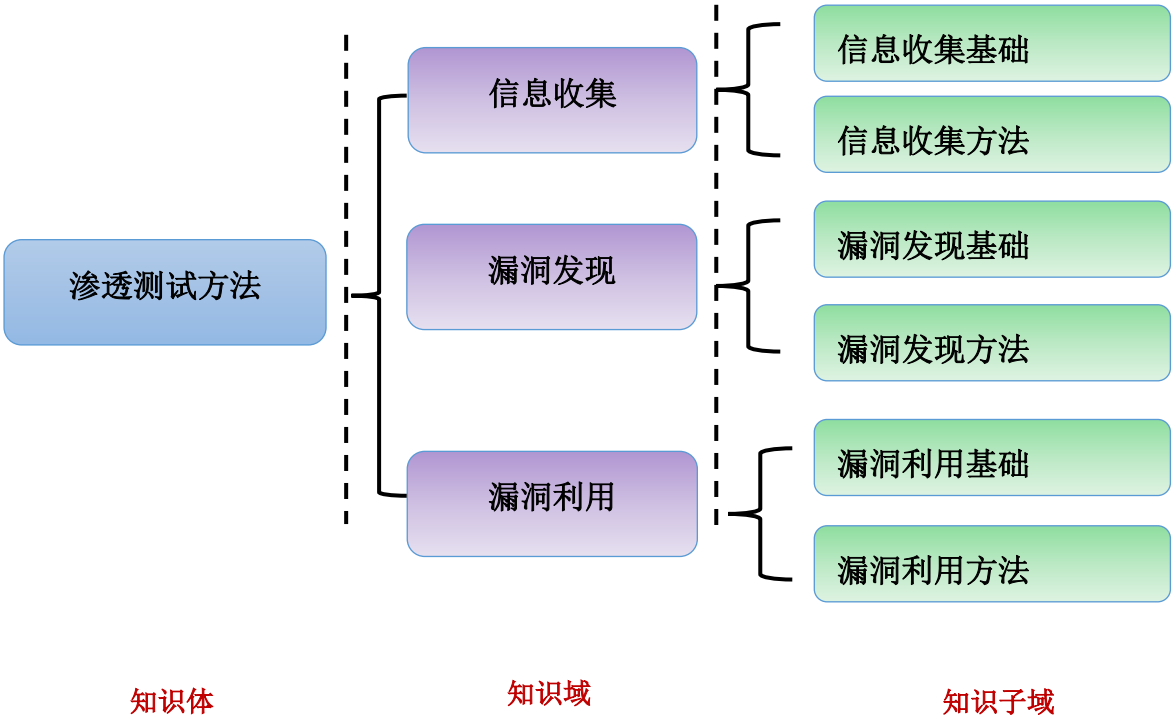

图 7-1：知识体：渗透测试方法

渗透测试是指渗透人员在不同的位置（比如从内网、从外网等位置）利用各种手段对某个特定网络进行测试，以期发现和挖掘系统中存在的漏洞，然后输出渗透测试报告，并提交给网络所有者。网络所有者根据渗透人员提供的渗透测试报告，可以清晰知晓系统中存在的安全隐患和问题。

7.1.1 知识域：信息收集

- 知识子域：信息收集基础
  - 了解信息收集的重要性
  - 了解收集信息的内容
- 知识子域：信息收集方法

- ◆ 了解信息收集的常用工具
- ◆ 掌握所收集信息的利用方法

7.1.2 知识域：漏洞发现

- 知识子域：漏洞发现基础
  - ◆ 了解通过信息收集发现的漏洞
  - ◆ 了解常用漏洞扫描工具
- 知识子域：漏洞发现方法
  - ◆ 了解漏洞发现工具的使用方法
  - ◆ 了解漏洞的验证与测试方法

7.1.3 知识域：漏洞利用

- 知识子域： 漏洞利用基础
  - ◆ 了解漏洞的原理
  - ◆ 了解漏洞的类型
- 知识子域： 漏洞利用方法
  - ◆ 了解漏洞利用的方式
  - ◆ 掌握如何利用漏洞获取权限