注册软件安全开发人员（CWASP CSSD）
知识体系大纲

版本：1.0

中国信息安全测评中心
广州闰业信息技术服务有限公司

目 录

前言

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及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。软件已成为运行各类业务和功能的载体，软件稳定可靠的运行是保障业务连续性和数据安全性最核心、也是最本根的因素。因此，软件开发过程中相关人员的信息安全意识、安全开发知识与技能已经成为保障软件系统安全稳定运行的重要前提条件之一。

注册软件安全开发人员（CWASP CSSD）是对我国网络基础设施和重要信息系统的软件开发人员进行资质评定的重要形式，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。

本大纲从国际主流的软件安全开发全生命周期理念与技术出发，结合我国软件开发安全保障和人才的实际需求，以知识体系的全面性和实用性为原则，明确规定了注册软件安全专业人员应当掌握的知识要点，是注册软件安全开发人员（CWASP CSSD）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：

1、注册软件安全开发人员（CWASP CSSD）知识体系概况

2、知识体：应用安全威胁

3、知识体：S-SDLC 流程

4、知识体：软件安全开发

1 注册软件安全开发人员（CWASP CSSD）知识体系概况

1.1 资质认定类别

注册软件安全专业人员（CWASP CSSP）系经中国信息安全测评中心认定的软件安全专业人员，是对我国网络信息系统软件开发人员安全开发能力实施的一种资质评定。

注册软件安全专业人员（CWASP CSSP）主要从事网络信息系统软件开发的相关工作，其具备一定的软件安全开发知识和技术，能在软件开发生命周期中提供必要的安全保障。

根据认证者的基础不同，注册软件安全开发人员（CWASP CSSP）共分为两种：

注册软件安全开发人员（Certified Secure Software Developer，简称 CWASP CSSD）。证书持有人员主要从事软件开发领域的工作。

注册软件安全专业人员（Certified Secure Software Professional，简称 CWASP CSSP）证书持有人员主要从事软件开发领域的技术与管理工作。

1.2 大纲范围

本大纲涵盖了注册软件安全开发人员（CWASP CSSD）需要掌握的知识要点。

1.3 注册软件安全开发人员（CWASP CSSD）知识体系框架结构

注册软件安全开发人员（CWASP CSSD）知识体系使用组件模块化的结构，包括知识体、知识域和知识子域三个层次。

（1） 知识体：对软件安全开发知识领域的总体划分，包含注册软件安全专业人员需要掌握的三大知识类别。知识体是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。

（2） 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。

（3） 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。

（1） 了解：是最低深度要求，学员只需要正确认识该知识要点的基本概念和原理。

（2） 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。

（3） 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。

在整个“注册软件安全开发人员（CWASP CSSD）”的知识体系结构中，共包括应用安全威胁、S-SDLC 流程和安全开发基本知识这三个知识体，每个知识体根据其逻辑划分为多个知识域，每个知识域由一个或多个知识子域组成。

注册软件安全开发人员（CWASP CSSD）知识体系结构共包含三个知识体，分别为：

（1） 应用安全威胁：主要介绍以“OWASP Top 10”为核心的应用安全威胁及应用安全威胁实例。

（2） S-SDLC 流程：主要介绍软件安全开发全生命周期的主要流程及安全管控措施。

（3） 软件安全开发：主要介绍软件开发过程中参数化查询、输出编码、输入验证、身份验证、访问控制等方面的技术知识和实践。这些是注册软件安全专业人员需要掌握的核心知识。

1.4 考试试题结构

注册软件安全开发人员（CWASP CSSD）考试题型均为单项选择题，共 100 题，每题 1 分，得到 70 分以上（含 70 分）为通过。

表格 1-1 中描述了 CWASP CSSD 各知识类试题的所占比例。

知识体	所占比例
应用安全威胁	50%
S-SDLC 流程	30%
软件安全开发	20%

2 知识体：应用安全威胁

“应用安全威胁”主要介绍以“OWASP Top 10”为核心的应用安全威胁及应用安全威胁实例。这些是“注册软件安全开发人员（CWASP CSSD）”首先需要掌握的常规知识。通过本部分的学习，学员应当：

- 理解 OWASP 组织研究形成的 10 大应用安全威胁的基本情况；
- 了解应用安全威胁可能造成的危害，提高应用安全的基本意识。

2.1 知识域：OWASP Top 10 应用安全威胁

2.1.1 知识子域：“注入”威胁

- 理解“注入”威胁的基本原理和造成的影响。
- 理解“注入”威胁的基本防范方法。
- 了解“注入”威胁的基本案例。

2.1.2 知识子域：“失效的身份认证和会话管理”威胁

- 理解“失效的身份认证和会话管理”威胁的基本原理和造成的影响。
- 理解“失效的身份认证和会话管理”威胁的基本防范方法。
- 了解“失效的身份认证和会话管理”威胁的基本案例。

2.1.3 知识子域：“跨站脚本（XSS）”威胁

- 理解“跨站脚本（XSS）”威胁的基本原理和造成的影响。
- 理解“跨站脚本（XSS）”威胁的基本防范方法。
- 了解“跨站脚本（XSS）”威胁的基本案例。

2.1.4 知识子域：“不安全的直接对象引用”威胁

- 理解“不安全的直接对象引用”威胁的基本原理和造成的影响。
- 理解“不安全的直接对象引用”威胁的基本防范方法。
- 了解“不安全的直接对象引用”威胁的基本案例。

2.1.5 知识子域：“安全配置错误”威胁

- 理解“安全配置错误”威胁的基本原理和造成的影响。
- 理解“安全配置错误”威胁的基本防范方法。
- 了解“安全配置错误”威胁的基本案例。

2.1.6 知识子域：“敏感信息泄露”威胁

- 理解“敏感信息泄露”威胁的基本原理和造成的影响。
- 理解“敏感信息泄露”威胁的基本防范方法。
- 了解“敏感信息泄露”威胁的基本案例。

2.1.7 知识子域：“功能级访问控制缺失”威胁

- 理解“功能级访问控制缺失”威胁的基本原理和造成的影响。
- 理解“功能级访问控制缺失”威胁的基本防范方法。
- 了解“功能级访问控制缺失”威胁的基本案例。

2.1.8 知识子域：“跨站请求伪造（CSRF）”威胁

- 理解“跨站请求伪造（CSRF）”威胁的基本原理和造成的影响。
- 理解“跨站请求伪造（CSRF）”威胁的基本防范方法。
- 了解“跨站请求伪造（CSRF）”威胁的基本案例。

2.1.9 知识子域：“使用含有已知漏洞的组件”威胁

- 理解“使用含有已知漏洞的组件”威胁的基本原理和造成的影响。
- 理解“使用含有已知漏洞的组件”威胁的基本防范方法。
- 了解“使用含有已知漏洞的组件”威胁的基本案例。

2.1.10 知识子域：“未验证的重定向和转发”威胁

- 理解“未验证的重定向和转发”威胁的基本原理和造成的影响。
- 理解“未验证的重定向和转发”威胁的基本防范方法。

- 了解“未验证的重定向和转发”威胁的基本案例。

2.2 知识域：应用安全威胁实例剖析

- 了解应用安全威胁造成的影响。
- 了解软件安全的重要性。

3 知识体：S-SDLC 流程

“S-SDLC 流程”技术是“注册软件安全专业人员（CWASP CSSD）”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：

- 理解 S-SDLC 软件安全开发全生命周期的流程及主要方法。

3.1 知识域：S-SDLC 需求阶段关键要素

- 掌握 S-SDLC 需求阶段的安全关键要素。

3.2 知识域：S-SDLC 设计阶段关键要素

- 掌握 S-SDLC 设计阶段的安全关键要素。

3.3 知识域：S-SDLC 实施阶段关键要素

- 掌握 S-SDLC 实施阶段的安全关键要素。

3.4 知识域：S-SDLC 验证阶段关键要素

- 掌握 S-SDLC 验证阶段的安全关键要素。

3.5 知识域：S-SDLC 发布与响应阶段关键要素

- 掌握 S-SDLC 发布与响应阶段的安全关键要素。

4 知识体：软件安全开发

软件安全开发是“注册软件安全开发人员（CWASP CSSD）”需要掌握的主体知识内容。通过本部分的学习，学员应当：

- 掌握输入验证、输出编码、访问控制、身份验证等方面软件安全开发技术的原理和基本实现方法；
- 掌握数据和隐私保护，实现日志、错误处理和入侵检测，利用框架的安全性和安全类库的原理和基本实现方法；

- 理解软件安全开发的主要方法。

4.1 知识域：输入验证

4.1.1 知识子域：输入验证的安全开发要求

- 了解输入验证的概念与作用。
- 掌握输入验证的主要安全开发要求。
- 了解如何防止注入。

4.1.2 知识子域：参考资源

- 了解 OWASP 安全组织提供的参考资源。

4.2 知识域： 输出编码

4.2.1 知识子域：输出编码的安全开发要求

- 了解输出编码的概念与作用。
- 掌握输出编码的主要安全开发要求。
- 了解常见输出编码技术。

4.2.2 知识子域：参考资源

- 了解 OWASP 安全组织提供的参考资源。

4.3 知识域：正确的实现访问控制

4.3.1 知识子域：访问控制

- 了解访问控制列表的概念和作用。
- 了解基于角色访问控制的概念和作用。

4.3.2 知识子域：访问控制的安全开发要求

- 掌握正确实现访问控制的原则。
- 掌握正确实现访问控制的主要安全开发要求。

4.3.3 知识子域：参考资源

- 了解 OWASP 安全组织提供的参考资源。

4.4 知识域：建立身份验证机制

4.4.1 知识子域：身份验证机制的安全开发要求

- 掌握建立身份验证机制的原则。
- 掌握建立身份验证机制的主要安全开发要求。

4.4.2 知识子域：参考资源

- 了解 OWASP 安全组织提供的参考资源。

4.5 知识域： 保护数据和隐私

4.5.1 知识子域：数据加密的安全开发要求

- 掌握数据加密的主要安全开发要求。

4.5.2 知识子域：数据保护的安全开发要求

- 掌握数据保护的主要安全开发要求。

4.5.3 知识子域：数据通讯的安全开发要求

- 掌握数据加密的主要安全开发要求。

4.5.4 知识子域：数据库的安全开发要求

- 掌握数据库的主要安全开发要求。

4.5.5 知识子域：文件管理的安全开发要求

- 掌握文件管理的主要安全开发要求。

4.5.6 知识子域：参考资源

- 了解 OWASP 安全组织提供的参考资源。

3.6 知识域：实现正确的日志和错误处理

3.6.1 知识子域：日志和错误处理的安全开发要求

- 掌握日志和错误处理的主要安全开发要求。

3.6.2 知识子域：参考资源

- 了解 OWASP 安全组织提供的参考资源。

3.7 知识域：利用框架的安全性和安全类库

3.7.1 知识子域：利用框架安全性和安全类库的原则

- 了解利用框架安全性和安全类库的原则。

3.7.2 知识子域：参考资源

- 了解 OWASP 安全组织提供的参考资源。