信息安全保障人员认证培训教材

# 软件安全开发

RUAN JIAN AN QUAN KAI FA

中国信息安全认证中心

◎主 编 张 剑 ◎副主编 丁 锋 周福才 于春刚

★★★ CISAW ★★★

电子科技大学出版社

信息安全保障人员认证培训教材

# 软件安全开发

RUAN JIAN AN QUAN KAI FA

中国信息安全认证中心

◎主 编 张 剑 ◎副主编 丁 锋 周福才 于春刚

★★★ CISAW ★★★

电子科技大学出版社

**图书在版编目（CIP）数据**

软件安全开发 / 张剑主编. —成都：电子科技大学出版社，2015.2

ISBN 978-7-5647-2853-3

Ⅰ. ①软… Ⅱ. ①张… Ⅲ. ①软件开发-安全技术 Ⅳ. ①TP311.52

中国版本图书馆 CIP 数据核字（2015）第 037901 号

## 内 容 提 要

本书从软件安全开发模型、漏洞管理、功能设计、常见问题、编码实践、安全测试等方面对软件安全开发进行讲解。软件安全开发模型部分重点介绍了几种典型的软件开发模型。安全漏洞管理部分从漏洞的概念、来源、分类以及等级等方面对漏洞的基础知识进行了详细介绍。安全功能设计过程主要参考欧美国家制定的《信息技术安全评估通用准则》和我国制定的《信息技术安全性评估准则》。常见安全问题和安全编码实践两章以问题案例的方式介绍了常见的安全编码问题及其解决方案，便于软件开发人员遇到相同问题时能够快速地分析出错原因。本书在软件安全测试一章中对软件安全测试方法、过程和组织进行了介绍，并给出了一个渗透测试的案例。

# 软件安全开发

**主　编**　张　剑

**副主编**　丁　锋　周福才

**出　　版**：电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦　邮编：610051）

**策划编辑**：徐守铭

**责任编辑**：郭蜀燕　徐守铭

**责任校对**：王　坤

**主　　页**：www.uestcp.com.cn

**电子邮箱**：uestcp@uestcp.com.cn

**发　　行**：新华书店经销

**印　　刷**：成都市川侨印务有限公司

**成品尺寸**：185 mm × 260 mm　　**印张** 19　　**字数** 390 千字

**版　　次**：2015 年 2 月第一版

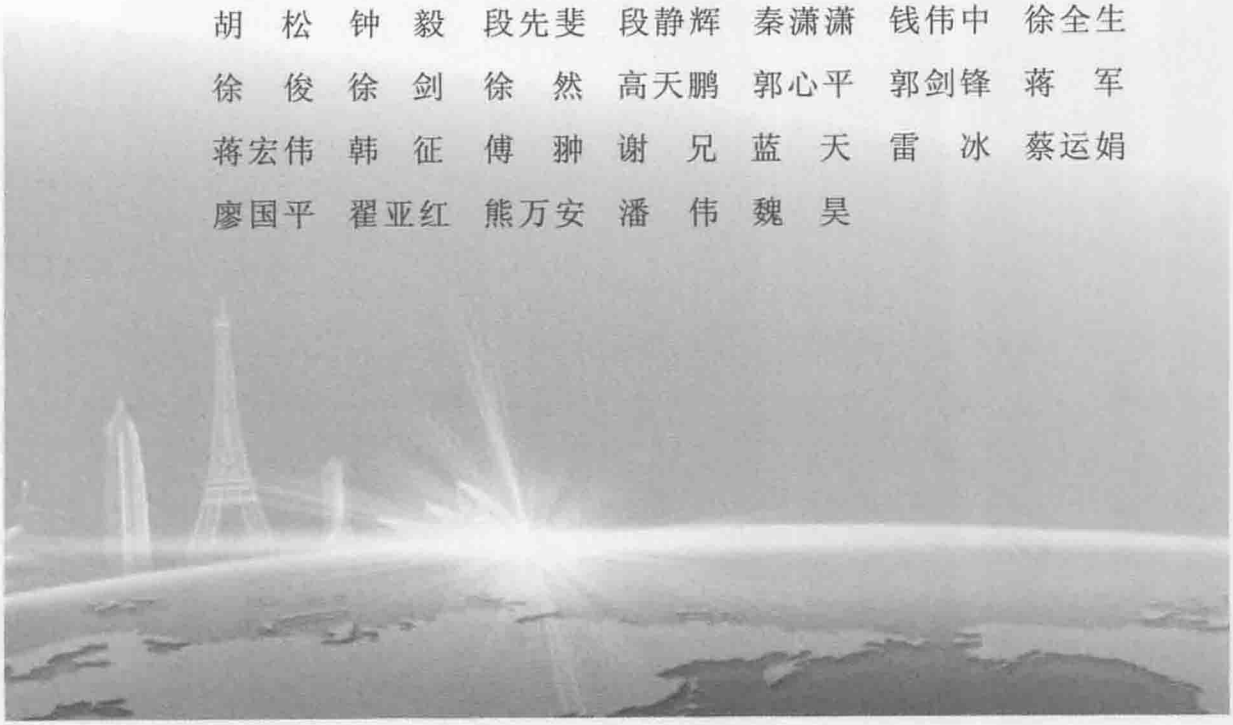
**印　　次**：2015 年 2 月第一次印刷

**书　　号**：ISBN 978-7-5647-2853-3

**定　　价**：50.00 元

# 丛书编委会





# 编 写 组


主　编　张　剑

副主编　丁　锋　周福才　于春刚

编　委　张维石　尹朝万　宋明秋　徐全生　郭剑锋　李　倩　张　雪

　　刘　洋　杨惟泓　岳笑含　林海峰　谢　兄　徐　剑　孙　爽


# 序

2014年，我国提出了建设网络强国战略与目标。实现网络强国，培养和造就网络与信息安全人才队伍是关键。据调查，截至2014年年底，国内网络与信息安全人才缺口高达50万人，并呈现持续增长的趋势。加快人才培养是我国经济社会发展和信息安全体系建设中的一项长期性、全局性和战略性的任务。

作为我国专业信息安全认证机构和培训机构，中国信息安全认证中心以保障国家网络与信息安全为己任，于2011年推出了信息安全保障人员认证（CISAW）。CISAW认证是面向IT从业人员、在校学生，特别是与网络与信息安全密切相关的高级管理人员、专业技术人员推出的人员资格认证和专业水平认证。CISAW认证的推出和实施，为培养和造就我国网络与信息安全人才探索了一条有效途径，得到了业内专家和社会各界的好评。

推行CISAW认证，编写高质量的教材尤为重要。鉴于此，中国信息安全认证中心组织国内信息安全保障的专业技术和应用领域的专家，依据《信息安全保障人员认证考试大纲》要求，结合信息安全保障工作的各岗位知识和应用能力要求，共同编著了信息安全保障人员认证系列教材。本系列教材包括《信息安全技术》《信息安全技术应用》和《信息安全实验》3种基础教材；《软件安全开发》《信息系统安全集成》《信息安全管理》《信息安全咨询手册》《信息系统安全运维》《信息系统安全审计》《信息安全风险管理》《网络攻防技术》《业务连续性管理》《云计算安全》《物联网安全》和《工业控制安全》12种专业技术应用教材；《电子政务安全》《电子商务安全》《交通服务信息安全》《能源服务信息安全》《医疗卫生信息安

全》《教育服务信息安全》《金融服务信息安全》《通信服务信息安全》《宾馆服务信息安全》和《物流服务信息安全》10种应用领域教材。

本系列教材以实用为首要原则，从统一的信息安全保障模型出发，构建了包括信息安全技术基础知识、信息安全专业技术知识和应用领域安全保障管理知识的完整信息安全保障知识体系。既是广大CISAW认证申请者的考试指导用书，同时也是广大信息安全保障工作者的工作指南和参考用书。

希望本系列教材的出版，能为广大信息安全保障从业者学习、工作和申请认证提供指导和帮助。

是为序。

中国信息安全认证中心主任　魏　昊

2014年12月28日

# 前　言

《软件安全开发》一书基于软件开发实践，在参考国内外同行的大量文献资料基础上，力图通过较小篇幅比较完整地、系统地介绍软件安全开发管理、技术与实践。本书从软件安全开发模型、安全漏洞管理、软件安全功能设计、常见安全问题、安全编码实践、软件安全测试共6个方面进行了系统的梳理与阐述。全书共7章，第1章在软件的定义和分类之后，主要给出了软件安全的范畴以及软件安全中的一些典型问题；第2章从软件安全开发模型和软件生命周期入手，重点介绍了几种典型的软件开发模型；第3章主要阐述了漏洞管理主要元素和流程、我国的漏洞管理机制、安全内容自动化协议、典型的软件安全漏洞等；第4章主要参考欧美国家制定的《信息技术安全评估通用准则》和我国制定的《信息技术安全性评估准则》，介绍软件安全功能设计；第5章重点介绍了软件安全设计中经常出现的编程安全问题，共列举66个安全编码问题，每个问题由问题描述、产生条件和问题涉及的编程语言3部分构成，供开发人员参考；第6章重点阐述如何实现安全的编码和安全编程实践知识；第7章对测试方法进行了系统的概述，对软件安全测试进行示例。

本书按照信息安全保障人员认证考试大纲的要求进行编著，适合广大申请认证考试的人员使用，同时也适合从事软件开发工作的软件技术人员、从事软件漏洞分析的安全人员以及学习安全软件课程的高等院校信息安全、计算机科学、软件工程类专业本科生和研究生使用。本书配套教程《信息安全技术》详细介绍了相关安全技术的基本概念和技术原理，可供相关人员参考。

本书由张剑、丁锋、周福才、于春刚、张维石、尹朝万、宋明秋、徐全生、郭剑锋、李倩、张雪、刘洋、杨惟泓、岳笑含、林海峰、谢兄、徐剑、孙爽等共同编写，在此，对各位的辛勤付出表示衷心感谢。

本书在成书过程中得到了《信息安全保障人员认证考试用书》编委会的指导，和中国信息安全认证中心、辽宁省信息安全与软件测评认证中心、四川省中认信安技术服务有限公司、四川亚和企业咨询管理有限公司、辽宁省信息技术教育中心及沈阳华信教育科技有限公司的大力支持，在此表示衷心感谢。

本书在编写过程中参考或引用了国内外同行的大量文献资料，在此向这些文献的作者表示衷心感谢。

本书力图比较完整地、系统地、正确地介绍软件安全相关的基本技术，但由于水平有限、时间紧迫，尽管我们进行了多次研讨和修订，书中仍难免存在疏漏和错误。在此，恳请广大读者和同行批评指正，以便我们再版修订时加以改正和完善。

张　剑

2014 年 12 月 18 日

# 目　录