



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美国国家制定的《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

■ 版权所有 侵权必究 ■

◆ 本社发行部电话: 028-83202463; 本社邮购电话: 028-83201495。

◆ 本书如有缺页、破损、装订错误, 请寄回印刷厂调换。

丛书编委会

主任 魏 昊

副主任 史小卫 陈晓桦 吴晓龙 亓明和

委员 (按姓氏笔画排序)

丁元汉	丁 锋	于春刚	万里冰	马卫东	王 刚	王怀宾
王 莉	王夏莲	王 强	王 静	亓明和	尹远飞	尹朝万
邓 刚	甘杰夫	史小卫	冯 丽	冯 峰	成林芳	朱灿庭
朱 强	华颜涛	刘春旺	刘春波	刘 洋 (广东)	刘 洋 (辽宁)	
刘润乾	汤志伟	孙 爽	杜孝伟	李 倩	李 源	杨惟泓
肖鸿江	吴永东	吴芳琼	吴晓龙	何一丁	宋 杨	宋明秋
张会平	张良龙	张 剑	张徐亮	张 雪	张维石	张 斌
陈 宇	陈晓桦	武 刚	林 利	林海峰	罗小兵	罗俊海
岳笑含	周佩雯	周福才	郑 莹	赵国庆	赵 洋	赵 辉
胡 松	钟 毅	段先斐	段静辉	秦潇潇	钱伟中	徐全生
徐 俊	徐 剑	徐 然	高天鹏	郭心平	郭剑锋	蒋 军
蒋宏伟	韩 征	傅 翀	谢 兄	蓝 天	雷 冰	蔡运娟
廖国平	翟亚红	熊万安	潘 伟	魏 昊		



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 CISA 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

第1章 软件安全概述	1
1.1 软件	1
1.1.1 软件定义	1
1.1.2 软件分类	1
1.2 软件安全	3
1.2.1 软件安全概述	3
1.2.2 软件安全范畴	4
1.2.3 软件安全问题	5
1.3 本书的结构与内容	10
第2章 软件安全开发模型	13
2.1 软件开发模型	13
2.1.1 瀑布型软件开发模型	13
2.1.2 渐增型软件开发模型	14
2.1.3 变换型软件开发模型	14
2.2 常用软件开发方法	15
2.2.1 结构化软件开发方法	15
2.2.2 面向对象的软件开发方法	15
2.2.3 组件开发方法	16
2.2.4 敏捷软件开发方法 (Scrum)	16
2.3 安全开发模型	17
2.4 微软安全开发生命周期模型	18
2.4.1 安全生命周期模型	18
2.4.2 SDL 优化模型	18
2.4.3 SDL 安全人员角色	19
2.4.4 SDL 模型安全活动	20

2.4.5	培训阶段	23
2.4.6	需求阶段	23
2.4.7	设计阶段	24
2.4.8	实施阶段	25
2.4.9	验证阶段	25
2.4.10	发布和响应阶段	26
2.4.11	可选的安全活动	27
2.5	McGraw 软件安全开发模型	28
2.5.1	代码审核 (工具)	30
2.5.2	体系结构风险分析	30
2.5.3	渗透测试	31
2.5.4	基于风险的安全测试	31
2.5.5	滥用用例	31
2.5.6	安全需求	31
2.5.7	安全操作	31
2.6	NIST 安全开发生命周期模型	32
2.6.1	开始阶段	33
2.6.2	获取与开发阶段	34
2.6.3	执行阶段	35
2.6.4	操作和维护阶段	36
2.6.5	部署阶段	36
2.7	CISAW 软件安全开发模型	37
2.7.1	对象	37
2.7.2	生命周期	38
2.7.3	安全属性	38
2.7.4	五个环节	38
2.7.5	资源	39
2.7.6	管理	39
第3章	安全漏洞管理	40
3.1	概述	40
3.1.1	漏洞分类	40
3.1.2	漏洞等级	42
3.1.3	漏洞管理流程	44
3.1.4	漏洞管理机制	45
3.2	安全内容自动化协议 (SCAP)	47

3.2.1	SCAP 及其元素	48
3.2.2	可扩展配置检查列表描述格式 XCCDF	50
3.2.3	开放漏洞评估描述语言 OVAL	50
3.2.4	通用漏洞和披露列表 CVE	51
3.2.5	通用平台枚举 CPE	51
3.2.6	通用配置枚举 CCE	52
3.2.7	通用漏洞评分系统 CVSS	53
3.3	典型软件安全漏洞	53
3.3.1	缓冲区溢出漏洞	54
3.3.2	整数溢出漏洞	57
3.3.3	格式化字符串漏洞	58
3.3.4	指针覆盖漏洞	61
3.3.5	SQL 注入漏洞	61
3.3.6	ByPass 漏洞	63
3.3.7	信息泄露漏洞	64
3.3.8	越权漏洞	64
3.4	OWASP Top 10	64
3.4.1	注入攻击	65
3.4.2	失效的身份认证和会话管理	67
3.4.3	跨站脚本 (XSS)	69
3.4.4	不安全的直接对象引用	71
3.4.5	安全配置错误	72
3.4.6	敏感数据暴露	74
3.4.7	功能级别访问控制缺失	75
3.4.8	跨站请求伪造 (CSRF)	77
3.4.9	使用已知易受攻击组件	78
3.4.10	未验证的重定向和转发	79
第 4 章	安全功能设计	81
4.1	安全审计	82
4.1.1	安全审计自动响应	83
4.1.2	安全审计数据产生	83
4.1.3	安全审计分析	84
4.1.4	安全审计查阅	86
4.1.5	安全审计事件选择	87
4.1.6	安全审计事件存储	87

4.2 安全通信	88
4.2.1 原发抗抵赖	89
4.2.2 接收抗抵赖	90
4.3 密码支持	92
4.3.1 密钥管理	93
4.3.2 密码运算	96
4.4 用户数据保护	97
4.4.1 访问控制	99
4.4.2 数据流控制	102
4.4.3 数据鉴别	105
4.4.4 系统内部传送	106
4.4.5 残余信息保护	108
4.4.6 回退	109
4.4.7 存储数据的完整性	110
4.5 标识和鉴别(身份认证)	111
4.5.1 用户鉴别	112
4.5.2 用户标识	114
4.5.3 鉴别失败	115
4.5.4 用户属性定义	115
4.5.5 秘密的规范	116
4.5.6 主体—用户绑定	117
4.6 安全管理	117
4.6.1 功能的管理	118
4.6.2 安全属性的管理	119
4.6.3 数据的管理	120
4.6.4 安全管理角色	121
4.7 隐私保护	122
4.7.1 匿名	123
4.7.2 假名	124
4.7.3 不可关联性	125
4.7.4 不可观察性	126
4.8 安全功能的保护	127
4.8.1 底层抽象机测试	129
4.8.2 失效保护	130
4.8.3 安全功能数据的可用性	131

4.8.4	安全功能数据的保密性	131
4.8.5	安全功能数据的完整性	132
4.8.6	内部数据传送	133
4.8.7	物理保护	134
4.8.8	可信恢复	136
4.8.9	重放检测	139
4.8.10	引用仲裁	139
4.8.11	域分离	141
4.8.12	状态同步协议	142
4.8.13	时间戳	143
4.8.14	对外数据一致性	143
4.8.15	内部数据复制一致性	144
4.8.16	安全功能自检	144
4.9	资源利用	145
4.9.1	容错	146
4.9.2	服务优先级	147
4.9.3	资源分配	148
4.10	系统/子系统的访问	149
4.10.1	可选属性范围限定	150
4.10.2	多重并发会话限定	150
4.10.3	会话锁定	151
4.10.4	访问旗标	153
4.10.5	访问历史	153
4.10.6	会话建立	154
4.11	可信路径/信道	155
4.11.1	安全功能之间的可信信道	155
4.11.2	可信路径	156
第5章	常见安全问题	157
5.1	概述	157
5.2	常见编程安全问题分类	157
5.3	常见编程安全问题	159
5.3.1	整数赋值错误问题	159
5.3.2	整型提升导致的内存溢出错误	160
5.3.3	临时变量溢出	160
5.3.4	整数截断错误问题	161

5.3.5	整数溢出问题	161
5.3.6	带符号与无符号整型比较问题	162
5.3.7	size_t 导致的死循环	162
5.3.8	误用 short 引起缓冲区溢出	163
5.3.9	表达式中对同一变量多次写入问题	164
5.3.10	空字符结尾错误问题	165
5.3.11	无界字符串复制问题	166
5.3.12	定长字符串越界问题	167
5.3.13	字符串截断问题	168
5.3.14	与函数无关的字符串错误问题	169
5.3.15	修改字符串常量错误问题	170
5.3.16	字符串比较错误	170
5.3.17	数组越界问题	172
5.3.18	数组定义和值初始化括号形式混淆错误	173
5.3.19	未正确区分标量和数组问题	173
5.3.20	二维数组的内存泄漏	174
5.3.21	释放指针指向的对象引起内存泄漏	175
5.3.22	数据指针被修改问题	176
5.3.23	函数指针被修改问题	177
5.3.24	删除 void * 指针错误	178
5.3.25	printf 函数输出问题	179
5.3.26	格式化函数 sprintf 引起缓冲区溢出	180
5.3.27	指针变量的传值和传址混淆问题	180
5.3.28	验证方法参数问题	181
5.3.29	函数退出时内存未释放问题	182
5.3.30	continue 和 return 混淆问题	183
5.3.31	非 void 返回类型函数问题	184
5.3.32	误用 sizeof 操作符取字符串长度	185
5.3.33	基类未定义虚析构函数引发错误	186
5.3.34	线程未 join 引起的内存泄漏	187
5.3.35	notify 线程唤醒问题	188
5.3.36	多线程中 Socket 终止问题	190
5.3.37	程序异常退出时未关闭已打开文件	192
5.3.38	目录打开后未关闭	193
5.3.39	写文件没有调用 fflush	193

5.3.40	临时文件未删除问题	194
5.3.41	敏感信息硬编码问题	196
5.3.42	引用未初始化的内存错误问题	197
5.3.43	检查和处理内存分配错误问题	198
5.3.44	执行零长度的分配错误问题	198
5.3.45	引用已释放内存的错误问题	199
5.3.46	双重释放内存错误问题	200
5.3.47	不匹配的内存管理函数问题	201
5.3.48	匿名对象引起的内存泄漏	201
5.3.49	JVM 内存泄漏问题	203
5.3.50	覆盖 equals 方法而没有覆盖 hashCode 方法问题	204
5.3.51	finally 程序段非正常退出问题	205
5.3.52	非泛型的数据类型问题	206
5.3.53	类名称比较问题	207
5.3.54	等同的对象得不到相等的结果问题	208
5.3.55	在嵌套类中暴露外部类的私有字段问题	209
5.3.56	静态方法隐藏问题	210
5.3.57	构造函数中抛出异常引发错误	211
5.3.58	构造器调用可覆盖方法问题	213
5.3.59	字符乱码问题	214
5.3.60	功能级别访问控制缺失问题	215
5.3.61	表单重复提交问题	217
5.3.62	不安全的直接对象引用问题	219
5.3.63	信息的不安全存储问题	220
5.3.64	SQL 注入攻击	220
5.3.65	失效的身份认证和会话管理问题	222
5.3.66	跨站脚本 (XSS)	223
第 6 章	安全编码实践	226
6.1	输入验证和数据合法性校验	226
6.1.1	输入数据有效性校验	226
6.1.2	避免 SQL 注入	227
6.1.3	避免 XML 注入	227
6.1.4	避免跨站脚本 (XSS)	228
6.2	声明和初始化	228
6.2.1	避免类初始化相互依赖	228

6.3 表达式	229
6.3.1 勿忽略方法返回值	229
6.3.2 勿引用空指针	230
6.3.3 比较数组内容	230
6.4 数值类型和操作	230
6.4.1 防止整数溢出	230
6.4.2 避免除法和取模运算分母为零	232
6.5 类和方法操作	232
6.5.1 数据成员声明为私有且提供可访问的包装方法	232
6.5.2 敏感类不允许复制	232
6.5.3 比较类的正确做法	233
6.5.4 不要硬编码敏感信息	233
6.5.5 验证方法参数	234
6.5.6 勿使用过时或低效的方法	234
6.5.7 数组引用问题	235
6.5.8 勿产生内存泄漏	235
6.6 异常处理	236
6.6.1 不要忽略捕获的异常	236
6.6.2 不允许暴露异常的敏感信息	237
6.6.3 不允许抛出 RuntimeException、Exception 和 Throwable	238
6.6.4 不要捕获 NullPointerException 或其他父类异常	239
6.7 多线程编程	240
6.7.1 确保被并发调用函数的可重入性	240
6.7.2 函数线程安全	242
6.7.3 确保共享变量的可见性	242
6.7.4 确保共享变量的操作是原子操作	244
6.7.5 Thread.run() 和 Thread.stop()	245
6.7.6 确保执行阻塞操作的线程可以终止	246
6.7.7 不在一个有限的线程池执行相互依存的任务	247
6.8 输入/输出	247
6.8.1 程序终止前删除临时文件	247
6.8.2 检测和处理文件相关错误	249
6.8.3 及时释放资源	249
6.9 序列化	250
6.9.1 不要序列化未加密的敏感数据	250