教育部高等学校网络空间安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

奇安信
新一代网络安全领军者

奇安信集团组织编写

网络空间安全重点规划丛书

顾问委员会主任：沈昌祥 编委会主任：封化民

Web安全原理分析与实践

闵海钊 李江涛 张敬 刘新鹏 编著

Cyberspace Security

根据教育部高等学校信息安全专业教学指导委员会编制的
《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

网络空间安全重点规划丛书

Web 安全原理分析与实践

闵海钊　李江涛　张　敬　刘新鹏　编著

清华大学出版社
北　京

内 容 简 介

本书全面介绍与 Web 安全相关的常见漏洞的原理分析和代码分析方法。全书共 13 章，第 1 章为 Web 安全基础，第 2～13 章讲述与 Web 安全相关的各类常见漏洞的原理分析与代码分析，涉及 SQL 注入漏洞、文件上传漏洞、文件包含漏洞、命令执行漏洞、代码执行漏洞、XSS 漏洞、SSRF 漏洞、XXE 漏洞、反序列化漏洞、中间件漏洞、解析漏洞、数据库漏洞，并分析了 Web 安全的攻击和防御方式。各章均提供了思考题。

本书适合作为信息安全、网络空间安全、网络工程等相关专业的教材，也可供网络安全运维人员、网络管理人员和对网络空间安全感兴趣的读者参考。

图书在版编目(CIP)数据

Web 安全原理分析与实践/闵海钊等编著. —北京：清华大学出版社，2019.9
(网络空间安全重点规划丛书)
ISBN 978-7-302-53769-4

Ⅰ. ①W…　Ⅱ. ①闵…　Ⅲ. ①互联网络－安全技术　Ⅳ. ①TP393.408

中国版本图书馆 CIP 数据核字(2019)第 201400 号

责任编辑：张　民　战晓雷
封面设计：常雪影
责任校对：时翠兰
责任印制：杨　艳

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954

印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张：**21.25　　**字　　数：**491 千字
版　　次：2019 年 11 月第 1 版　　**印　　次：**2019 年 11 月第1 次印刷
定　　价：55.00 元

产品编号：085204-01

网络空间安全重点规划丛书

编审委员会

出版说明

21 世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继 2001 年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量具有前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。系列教材的作者都是既在本专业领域有深厚的学术造诣，又在教学第一线有丰富的教学经验的学者、专家。

该系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入系列教材中，以进一步满足大家对外版书的需求。“高等院校信息安全专业系列教材”已于 2006 年年初正式列入普通高等教育“十一五”国家级教材规划。

2007 年 6 月，教育部高等学校信息安全类专业教学指导委员会成立大会

暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展起到重要的指导和推动作用。2006 年教育部给武汉大学下达了“信息安全专业指导性专业规范研制”的教学科研项目。2007 年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下，项目组团结一致，努力工作，克服困难，历时 5 年，制定出我国第一个信息安全专业指导性专业规范，于 2012 年年底通过经教育部高等教育司理工科教育处授权组织的专家组评审，并且已经得到武汉大学等许多高校的实际使用。2013 年，新一届教育部高等学校信息安全专业教学指导委员会成立。经组织审查和研究决定，2014 年以教育部高等学校信息安全专业教学指导委员会的名义正式发布《高等学校信息安全专业指导性专业规范》(由清华大学出版社正式出版)。

2015 年 6 月，国务院学位委员会、教育部出台增设“网络空间安全”为一级学科的决定，将高校培养网络空间安全人才提到新的高度。2016 年 6 月，中央网络安全和信息化领导小组办公室(下文简称中央网信办)、国家发展和改革委员会、教育部、科学技术部、工业和信息化部及人力资源和社会保障部六大部门联合发布《关于加强网络安全学科建设和人才培养的意见》(中网办发文〔2016〕4 号)。2019 年 6 月，教育部高等学校网络空间安全专业教学指导委员会召开成立大会。为贯彻落实《关于加强网络安全学科建设和人才培养的意见》，进一步深化高等教育教学改革，促进网络安全学科专业建设和人才培养，促进网络空间安全相关核心课程和教材建设，在教育部高等学校网络空间安全专业教学指导委员会和中央网信办资助的网络空间安全教材建设课题组的指导下，启动了“网络空间安全重点规划丛书”的工作，由教育部高等学校网络空间安全专业教学指导委员会秘书长封化民教授担任编委会主任。本规划丛书基于“高等院校信息安全专业系列教材”坚实的工作基础和成果、阵容强大的编审委员会和优秀的作者队伍，目前已经有多本图书获得教育部和中央网信办等机构评选的“普通高等教育本科国家级规划教材”“普通高等教育精品教材”“中国大学出版社图书奖”和“国家网络安全优秀教材奖”等多个奖项。

“网络空间安全重点规划丛书”将根据《高等学校信息安全专业指导性专业规范》(及后续版本)和相关教材建设课题组的研究成果不断更新和扩展，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国网络空间安全学科的发展不断完善，力争为我国网络空间安全相关学科专业的本科和研究生教材建设、学术出版与人才培养做出更大的贡献。

我们的 E-mail 地址是：zhangm@tup.tsinghua.edu.cn，联系人：张民。

“网络空间安全重点规划丛书”编审委员会

前 言

没有网络安全，就没有国家安全；没有网络安全人才，就没有网络安全。

为了更多、更快、更好地培养网络安全人才，许多高校都在加大投入，聘请优秀教师，招收优秀学生，以建设一流的网络空间安全专业。

网络空间安全专业建设需要体系化的培养方案、系统化的专业教材和专业化的师资队伍。优秀教材是网络空间安全专业人才培养的关键，然而，这是一项十分艰巨的任务。原因有二：其一，网络空间安全的涉及面非常广，至少包括密码学、数学、计算机、通信工程等多门学科，因此，其知识体系庞杂，难以梳理；其二，网络空间安全的实践性很强，技术发展更新非常快，对教学环境和师资要求也很高。

作者一直从事网络安全方面的教学、服务和研究工作，积累了大量的实践经验。通过本书，作者将自己积累的学习经验和实际工作中的实践经验与读者分享，使读者可以在 Web 安全领域快速入门，通过典型漏洞代码分析对 Web 安全的漏洞原理有深入的理解，并且通过案例实践提高实际操作能力。

本书对各种漏洞的形成原理进行了深入、详细的分析，既包括常见的经典漏洞，也包括近来出现的新型漏洞，对各种漏洞都结合案例进行了详细的代码分析，并对漏洞的利用方式进行了全面讲解。读者可以通过本书了解各种漏洞的形成原理、利用方式及修复方法。不论是初学者还是有一定工作经验的从业者，都能通过本书全面、系统地掌握漏洞原理和相关知识。本书既可以作为 Web 安全初学者的入门书籍，又可以作为 Web 安全工作者的工具书。

“Web 安全原理分析与实践”是网络空间安全和信息安全专业的专业课程。本书由浅入深，由理论到实践，讲解了与 Web 攻防相关的整个体系，涉及的知识面很宽。本书共 13 章。第 1 章介绍 Web 安全基础，第 2 章介绍 SQL 注入漏洞，第 3 章介绍文件上传漏洞，第 4 章介绍文件包含漏洞，第 5 章介绍命令执行漏洞，第 6 章介绍代码执行漏洞，第 7 章介绍 XSS 漏洞，第 8 章介绍 SSRF 漏洞，第 9 章介绍 XXE 漏洞，第 10 章介绍反序列化漏洞，第 11 章介绍中间件漏洞，第 12 章介绍解析漏洞，第 13 章介绍数据库漏洞。

本书既适合作为高校网络空间安全、信息安全、网络工程等相关专业的教材，也适合作为网络空间安全研究人员的基础读物。随着新技术的不断发展，作者今后将不断更新本书内容。

本书主要由闵海钊编写，参与编写的人员有李江涛、张敬、刘新鹏，参与

校阅书稿的人员有张燕飞、王萌。本书的完成离不开作者的亲人和朋友的支持。在此我要感谢父母的养育之恩，是他们含辛茹苦把我养育成人；感谢参与编写和校阅的同事和朋友；感谢公司和领导对我的培养，给我成长、锻炼的机会；感谢清华大学出版社的编辑，他们给了我很多专业的建议和帮助；感谢所有对本书做出贡献的人，没有他们的付出和支持，本书不可能面世。

特别说明：本书中使用的每一个 URL 或者 IP 地址都是作者自己搭建的测试环境地址，如果与已有的域名或者 IP 地址重复，纯属巧合。本书相关的漏洞示例代码和相关工具的下载方式统一放在清华大学出版社官网的本书页面。

本书大部分内容是作者利用业余时间在实践的基础上编写的。由于时间仓促，书中难免存在疏漏和不妥之处，欢迎读者批评指正。

不忘初心，方得始终。

闵海钊

2019 年 6 月

目 录