Web 攻防之
业务安全实战指南

陈晓光 胡兵 张作峰 等编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

业务安全漏洞作为常见的 Web 安全漏洞，在各大漏洞平台时有报道，本书是一本从原理到案例分析，系统性地介绍这门技术的书籍。撰写团队具有 10 年大型网站业务安全测试经验，成员们对常见业务安全漏洞进行梳理，总结出了全面、详细的适用于电商、银行、金融、证券、保险、游戏、社交、招聘等业务系统的测试理论、工具、方法及案例。

本书共 15 章，包括理论篇、技术篇和实践篇。理论篇首先介绍从事网络安全工作涉及的相关法律法规，请大家一定要做一个遵纪守法的白帽子，然后介绍业务安全引发的一些安全问题和业务安全测试相关的方法论，以及怎么去学好业务安全。技术篇和实践篇选取的内容都是这些白帽子多年在电商、金融、证券、保险、游戏、社交、招聘、O2O 等不同行业、不同的业务系统存在的各种类型业务逻辑漏洞进行安全测试总结而成的，能够帮助读者理解不同行业的业务系统涉及的业务安全漏洞的特点。具体来说，技术篇主要介绍登录认证模块测试、业务办理模块测试、业务授权访问模块测试、输入/输出模块测试、回退模块测试、验证码机制测试、业务数据安全测试、业务流程乱序测试、密码找回模块测试、业务接口模块调用测试等内容。实践篇主要针对技术篇中的测试方法进行相关典型案例的测试总结，包括账号安全案例总结、密码找回案例总结、越权访问案例、OAuth 2.0 案例总结、在线支付安全案例总结等。

通过对本书的学习，读者可以很好地掌握业务安全层面的安全测试技术，并且可以协助企业规避业务安全层面的安全风险。本书比较适合作为企业专职安全人员、研发人员、普通高等院校网络空间安全学科的教学用书和参考书，以及作为网络安全爱好者的自学用书。

图书在版编目（CIP）数据

Web 攻防之业务安全实战指南 / 陈晓光等编著. —北京：电子工业出版社，2018.3
ISBN 978-7-121-33581-5

Ⅰ. ①W… Ⅱ. ①陈… Ⅲ. ①互联网络－安全技术－指南 Ⅳ. ①TP393.408-62

中国版本图书馆 CIP 数据核字（2018）第 019878 号

责任编辑：董　英
印　　刷：三河市双峰印刷装订有限公司
装　　订：三河市双峰印刷装订有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编　100036
开　　本：787×980　1/16　印张：17.5　字数：292 千字
版　　次：2018 年 3 月第 1 版
印　　次：2018 年 3 月第 1 次印刷
定　　价：69.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）51260888-819，faq@phei.com.cn。

前　言

“没有网络安全就没有国家安全”。当前，网络安全已被提升到国家战略的高度，成为影响国家安全、社会稳定至关重要的因素之一。

由于 Web 2.0 的兴起，基于 Web 环境的互联网应用越来越广泛，也让 Web 应用的安全技术日趋成熟。目前互联网上接连爆发的应用安全漏洞，让各大企业的安全人员、运维人员、研发及管理人员都不得不重视这一领域，并为之投入了大量的人力和物力。日渐成熟的防护产品和解决方案，让 Web 安全防护的整体环境有了很大的提升。互联网上的网站模板，大部分都自带了防 SQL 注入、跨站脚本等攻击的功能，传统的“工具党”、“小白”已很难再通过简单操作几个按钮就成功完成一次 Web 入侵。

随着互联网业务的不断发展，互联网上的商务活动也越来越多，所涉及的网络交易也越来越频繁，交易的数额也越来越庞大，引发的安全事件也越来越多。而这些安全事件的攻击者更倾向于利用业务逻辑层的安全漏洞，如互联网上曝光的“1 元购买特斯拉”、“微信无限刷红包”、“支付宝熟人可重置登录密码”等业务安全层面的漏洞。基于传统的渗透测试方法很难发现这些业务逻辑层面的问题，这类问题往往又危害巨大，可能造成企业的资产损失和名誉受损，并且传统的安全防御设备和措施对业务安全漏洞防护收效甚微。

业务安全问题在互联网上也时有报道，不算新生事物，但目前缺乏一套体系化的介绍这门技术的书籍。我们通过多年的不同行业的安全服务经验积累了大量的业务安全方面的经验，于是萌生了编写这本书的想法，把我们所有沉淀的业务安全测试经验分享给爱好网络安全事业的白帽子们，让大家一起成长，共同为国家网络安

全事业贡献绵薄之力。

本书的撰写者均为轩辕攻防实验室白帽子，这些白帽子具备多年的业务安全测试经验，同时他们在国家信息安全漏洞共享平台（CNVD）报送过很多原创漏洞（2016年轩辕攻防实验室报送原创漏洞排名第二）。这些白帽子平时低调做人、高调做事，听说要编写这本书时，大家群情激奋，热烈响应，牺牲了很多的个人休息时间，经过了近一年的努力才总结完成了全面的、详细的可以适用于不同行业和不同业务系统的业务安全测试理论、工具、方法及案例。在此也感谢所有参与撰写本书的这些默默无闻，不求名、不逐利、默默分享的白帽子。在编写本书的过程中，我们也在互联网上发现了很多关于业务安全方面的经典案例，并选取了几个非常不错且比较典型的案例，经过我们整理总结后分享给各位读者，有的案例原作者已经联系上了，有个别的也无从联系了，在此也对分享这些经典案例且默默在互联网上耕耘和贡献的白帽子表示衷心的感谢和发自内心的致敬。

在内容甄选时，抛开了一些纯理论的内容，书中选取的场景案例多是作者在工作中实际遇到的问题加以改造的，目的是让读者通过对本书的学习，掌握实用的业务安全测试技术，协助企业规避业务安全层面的安全风险。

本书共 15 章，包括理论篇、技术篇和实践篇。理论篇开篇首先介绍从事网络安全工作涉及的相关法律法规，请大家一定要做一个遵纪守法的白帽子，然后介绍业务安全引发的一些安全问题和业务安全测试相关的方法论及怎么去学好业务安全。技术篇和实践篇选取的内容都是这些白帽子多年在电商、金融、证券、保险、游戏、社交、招聘、O2O 等不同行业、不同的业务系统存在的各种类型业务逻辑漏洞进行安全测试总结而成的，能够帮助读者理解不同行业的业务系统涉及的业务安全漏洞的特点。具体来说，技术篇主要介绍登录认证模块测试、业务办理模块测试、业务授权访问模块测试、输入/输出模块测试、回退模块测试、验证码机制测试、业务数据安全测试、业务流程乱序测试、密码找回模块测试、业务接口模块调用测试等内容。实践篇主要针对技术篇中的测试方法进行相关典型案例的测试总结，包括账号安全案例总结、密码找回案例总结、越权访问案例、OAuth 2.0 案例总结、在线支付安全案例总结等。

通过对本书的学习读者可以很好地掌握业务安全层面的安全测试技术，并且可以协助企业规避业务安全层面的安全风险。本书比较适合作为企业专职安全人员、研发人员、普通高等院校网络空间安全学科的教学用书和参考书，以及作为网络安全爱好者的自学用书。

由于水平有限，书中难免有不妥之处，加之网络攻防技术纵深宽广，发展迅速，在内容取舍和编排上难免考虑不周全，诚请读者批评指正。

参与本书编写的还有：卜宁琳、袁溟森、刘书、陈亮亮、程利明、黄泽超、吉驰、闫石坚、杨志学、张冠廷、张瑜龙、陈明、陈延飞、杨梦端。

轩辕攻防实验室负责人　张作峰

2018 年 01 月　于北京

轻松注册成为博文视点社区用户（www.broadview.com.cn），扫码直达本书页面。

- **提交勘误**：您对书中内容的修改意见可在 提交勘误 处提交，若被采纳，将获赠博文视点社区积分（在您购买电子书时，积分可用来抵扣相应金额）。
- **交流互动**：在页面下方 读者评论 处留下您的疑问或观点，与我们和其他读者一同学习交流。

页面入口：http://www.broadview.com.cn/33581

致　谢

在出版之际，对关心和支持我们的所有朋友表示衷心的感谢。

感谢恒安嘉新（北京）科技股份公司金红董事长对编写工作的支持。

感谢中国联合网络通信有限公司信息化部林海对本书的审核和指导。

感谢国家互联网应急中心网络安全处主任严寒冰、公安部第三研究所主任徐凯、中国信息安全测评中心系统评估处任望、威客安全 CEO 陈新龙、Joinsec 创始人余弦、360 补天漏洞响应平台负责人白健、漏洞盒子创始人袁劲松的推荐语，他们是业界的标杆和大家学习的楷模。

感谢一直给予我们帮助和鼓励的同事和朋友们，他们包括但不限于：吕雪梅、刘晓蔚、刘宏杰、王小华、王幼平、赵岳磊、王兆龙、郭铁城、毛华均、胡付博、刘新鹏、金健杨等。

最后感谢互联网上默默耕耘的白帽子刘欢、horseluke、only_guest、px1624、汉时明月、牛奶坦克、猪哥靓、savior、0x 80、Rocky.Tian 等业内人士对安全攻防技术的分享。

目　录

理论篇

技术篇

实践篇