

Web攻防之业务安全实战指南



[Web攻防之业务安全实战指南_下载链接1](#)

著者:陈晓光

出版者:电子工业出版社

出版时间:2018-3

装帧:

isbn:9787121335815

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，《Web攻防之业务安全实战指南》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。

《Web攻防之业务安全实战指南》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《Web攻防之业务安全实战指南》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。《Web攻防之业务安全实战指南》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。

作者介绍:

陈晓光

恒安嘉新（北京）科技股份有限公司执行总裁，资深安全专家，毕业于北京邮电大学信息安全专业。长期从事网络与信息安全方面的技术研究、项目管理和市场拓展工作。曾主导和参与多项重大国家标准、国家863项目和242安全课题；建设了多个全国性安全系统工程；为电信、金融和政府等多个行业提供安全建议。在安全风险评估、安全管理体系、安全标准、移动互联网安全和通信安全等领域有着丰富的实践经验。拥有CISSP、CISA、ISO27001 LA等多项国际安全从业资质。

胡兵恒

安嘉新（北京）科技股份有限公司安全攻防与应急响应中心总经理。负责公司安全产品解决方案、安全攻防技术研究、安全咨询服务等工作。多年来，一直致力于安全攻防技术的研究，曾参与国家信息安全有关部门、各大电信运营商、高校多个课题研究项目。带领安全研究团队支撑“中国反网络病毒联盟平台ANVA”、“国家信息安全漏洞共享平台CVD”运营工作，以及承担国家重要活动期间的安全保障工作。

张作峰（Rce）

恒安嘉新（北京）科技股份有限公司安全攻防与应急响应中心副总经理、轩辕攻防实验室团队负责人、安全专家、互联网白帽子，原启明星辰资深安全研究员。十余年网络安全服务、安全研究、应急保障工作经验，在职期间参与完成了多个大型安全服务、集成、安全课题项目，以及多次国家重要活动的网络安全应急保障任务。

目录: 理论篇

第1章 网络安全法律法规 2

第2章 业务安全引发的思考 8

2.1 行业安全问题的思考 8

2.2 如何更好地学习业务安全 9

第3章 业务安全测试理论 11

3.1 业务安全测试概述	11
3.2 业务安全测试模型	12
3.3 业务安全测试流程	13
3.4 业务安全测试参考标准	18
3.5 业务安全测试要点	18
技术篇	
第4章 登录认证模块测试	22
4.1 暴力破解测试	22
4.1.1 测试原理和方法	22
4.1.2 测试过程	22
4.1.3 修复建议	30
4.2 本地加密传输测试	30
4.2.1 测试原理和方法	30
4.2.2 测试过程	30
4.2.3 修复建议	32
4.3 Session测试	32
4.3.1 Session会话固定测试	32
4.3.2 Seesion会话注销测试	35
4.3.3 Seesion会话超时时间测试	39
4.4 Cookie仿冒测试	42
4.4.1 测试原理和方法	42
4.4.2 测试过程	42
4.4.3 修复建议	45
4.5 密文比对认证测试	45
4.5.1 测试原理和方法	45
4.5.2 测试过程	45
4.5.3 修复建议	48
4.6 登录失败信息测试	48
4.6.1 测试原理和方法	48
4.6.2 测试过程	49
4.6.3 修复建议	50
第5章 业务办理模块测试	51
5.1 订单ID篡改测试	51
5.1.1 测试原理和方法	51
5.1.2 测试过程	51
5.1.3 修复建议	55
5.2 手机号码篡改测试	55
5.2.1 测试原理和方法	55
5.2.2 测试过程	56
5.2.3 修复建议	57
5.3 用户ID篡改测试	58
5.3.1 测试原理和方法	58
5.3.2 测试过程	58
5.3.3 修复建议	60
5.4 邮箱和用户篡改测试	60
5.4.1 测试原理和方法	60
5.4.2 测试过程	61
5.4.3 修复建议	62
5.5 商品编号篡改测试	63
5.5.1 测试原理和方法	63
5.5.2 测试过程	63
5.5.3 修复建议	65
5.6 竞争条件测试	66
5.6.1 测试原理和方法	66

5.6.2 测试过程	67
5.6.3 修复建议	69
第6章 业务授权访问模块	70
6.1 非授权访问测试	70
6.1.1 测试原理和方法	70
6.1.2 测试过程	70
6.1.3 修复建议	71
6.2 越权测试	72
6.2.1 测试原理和方法	72
6.2.2 测试过程	72
6.2.3 修复建议	76
第7章 输入/输出模块测试	77
7.1 SQL注入测试	77
7.1.1 测试原理和方法	77
7.1.2 测试过程	78
7.1.3 修复建议	84
7.2 XSS测试	84
7.2.1 测试原理和方法	84
7.2.2 测试过程	85
7.2.3 修复建议	88
7.3 命令执行测试	89
7.3.1 测试原理和方法	89
7.3.2 测试过程	89
7.3.3 修复建议	91
第8章 回退模块测试	92
8.1 回退测试	92
8.1.1 测试原理和方法	92
8.1.2 测试过程	92
8.1.3 修复建议	93
第9章 验证码机制测试	94
9.1 验证码暴力破解测试	94
9.1.1 测试原理和方法	94
9.1.2 测试过程	94
9.1.3 修复建议	97
9.2 验证码重复使用测试	97
9.2.1 测试原理和方法	97
9.2.2 测试过程	98
9.2.3 修复建议	100
9.3 验证码客户端回显测试	101
9.3.1 测试原理和方法	101
9.3.2 测试过程	101
9.3.3 修复建议	104
9.4 验证码绕过测试	104
9.4.1 测试原理和方法	104
9.4.2 测试过程	104
9.4.3 修复建议	106
9.5 验证码自动识别测试	106
9.5.1 测试原理和方法	106
9.5.2 测试过程	107
9.5.3 修复建议	111
第10章 业务数据安全测试	112
10.1 商品支付金额篡改测试	112
10.1.1 测试原理和方法	112
10.1.2 测试过程	112

- 10.1.3 修复建议 115
- 10.2 商品订购数量篡改测试 115
 - 10.2.1 测试原理和方法 115
 - 10.2.2 测试过程 115
 - 10.2.3 修复建议 120
- 10.3 前端JS限制绕过测试 121
 - 10.3.1 测试原理和方法 121
 - 10.3.2 测试过程 121
 - 10.3.3 修复建议 123
- 10.4 请求重放测试 123
 - 10.4.1 测试原理和方法 123
 - 10.4.2 测试过程 123
 - 10.4.3 修复建议 125
- 10.5 业务上限测试 126
 - 10.5.1 测试原理和方法 126
 - 10.5.2 测试过程 126
 - 10.5.3 修复建议 128
- 第11章 业务流程乱序测试 129
 - 11.1 业务流程绕过测试 129
 - 11.1.1 测试原理和方法 129
 - 11.1.2 测试过程 129
 - 11.1.3 修复建议 133
- 第12章 密码找回模块测试 134
 - 12.1 验证码客户端回显测试 134
 - 12.1.1 测试原理和方法 134
 - 12.1.2 测试流程 134
 - 12.1.3 修复建议 137
 - 12.2 验证码暴力破解测试 137
 - 12.2.1 测试原理和方法 137
 - 12.2.2 测试流程 137
 - 12.2.3 修复建议 140
 - 12.3 接口参数账号修改测试 140
 - 12.3.1 测试原理和方法 140
 - 12.3.2 测试流程 141
 - 12.3.3 修复建议 144
 - 12.4 Response状态值修改测试 144
 - 12.4.1 测试原理和方法 144
 - 12.4.2 测试流程 144
 - 12.4.3 修复建议 147
 - 12.5 Session覆盖测试 147
 - 12.5.1 测试原理和方法 147
 - 12.5.2 测试流程 148
 - 12.5.3 修复建议 150
 - 12.6 弱Token设计缺陷测试 150
 - 12.6.1 测试原理和方法 150
 - 12.6.2 测试流程 151
 - 12.6.3 修复建议 153
 - 12.7 密码找回流程绕过测试 153
 - 12.7.1 测试原理和方法 153
 - 12.7.2 测试流程 154
 - 12.7.3 修复建议 157
- 第13章 业务接口调用模块测试 158
 - 13.1 接口调用重放测试 158
 - 13.1.1 测试原理和方法 158

13.1.2 测试过程	158
13.1.3 修复建议	160
13.2 接口调用遍历测试	160
13.2.1 测试原理和方法	160
13.2.2 测试过程	161
13.2.3 修复建议	166
13.3 接口调用参数篡改测试	167
13.3.1 测试原理和方法	167
13.3.2 测试过程	167
13.3.3 修复建议	169
13.4 接口未授权访问/调用测试	169
13.4.1 测试原理和方法	169
13.4.2 测试过程	170
13.4.3 修复建议	172
13.5 Callback自定义测试	172
13.5.1 测试原理和方法	172
13.5.2 测试过程	173
13.5.3 修复建议	177
13.6 Webservice测试	177
13.6.1 测试原理和方法	177
13.6.2 测试过程	177
13.6.3 修复建议	184
实践篇	
第14章 账号安全案例总结	186
14.1 账号安全归纳	186
14.2 账号安全相关案例	187
14.1.1 账号密码直接暴露在互联网上	187
14.1.2 无限制登录任意账号	189
14.1.3 电子邮件账号泄露事件	192
14.1.4 中间人攻击	195
14.1.5 撞库攻击	197
14.3 防范账号泄露的相关手段	199
第15章 密码找回安全案例总结	200
15.1 密码找回凭证可被暴力破解	200
15.1.1 某社交软件任意密码修改案例	201
15.2 密码找回凭证直接返回给客户端	203
15.2.1 密码找回凭证暴露在请求链接中	204
15.2.2 加密验证字符串返回给客户端	205
15.2.3 网页源代码中隐藏着密保答案	206
15.2.4 短信验证码返回给客户端	207
15.3 密码重置链接存在弱Token	209
15.3.1 使用时间戳的md5作为密码重置Token	209
15.3.2 使用服务器时间作为密码重置Token	210
15.4 密码重置凭证与用户账户关联不严	211
15.4.1 使用短信验证码找回密码	212
15.4.2 使用邮箱Token找回密码	213
15.5 重新绑定用户手机或邮箱	213
15.5.1 重新绑定用户手机	214
15.5.2 重新绑定用户邮箱	215
15.6 服务端验证逻辑缺陷	216
15.6.1 删除参数绕过验证	217
15.6.2 邮箱地址可被操控	218
15.6.3 身份验证步骤可被绕过	219
15.7 在本地验证服务端的返回信息——修改返回包绕过验证	221

- 15.8 注册覆盖——已存在用户可被重复注册 222
- 15.9 Session覆盖——某电商网站可通过Session覆盖方式重置他人密码 223
- 15.10 防范密码找回漏洞的相关手段 225
- 第16章 越权访问安全案例总结 227
 - 16.1 平行越权 227
 - 16.1.1 某高校教务系统用户可越权查看其他用户个人信息 227
 - 16.1.2 某电商网站用户可越权查看或修改其他用户信息 229
 - 16.1.3 某手机APP普通用户可越权查看其他用户个人信息 232
 - 16.2 纵向越权 233
 - 16.2.1 某办公系统普通用户权限越权提升为系统权限 233
 - 16.2.2 某中学网站管理后台可越权添加管理员账号 235
 - 16.2.3 某智能机顶盒低权限用户可越权修改超级管理员配置信息 240
 - 16.2.4 某Web防火墙通过修改用户对菜单类别可提升权限 244
 - 16.3 防范越权访问漏洞的相关手段 247
- 第17章 OAuth 2.0安全案例总结 248
 - 17.1 OAuth 2.0认证原理 248
 - 17.2 OAuth 2.0漏洞总结 250
 - 17.2.1 某社交网站CSRF漏洞导致绑定劫持 250
 - 17.2.2 某社区劫持授权 251
 - 17.3 防范OAuth 2.0漏洞的相关手段 253
- 第18章 在线支付安全案例总结 254
 - 18.1 某快餐连锁店官网订单金额篡改 254
 - 18.2 某网上商城订单数量篡改 256
 - 18.3 某服务器供应商平台订单请求重放测试 257
 - 18.4 某培训机构官网订单其他参数干扰测试 259
 - 18.5 防范在线支付漏洞的相关手段 261
 - • • • • [\(收起\)](#)

[Web攻防之业务安全实战指南_下载链接1](#)

标签

web安全

黑客

安全

渗透测试

评论

了解下

不到两个小时看完全书。大量的burp配图扩充了页码数。大部分案例是常规手段。全是梳理了一下逻辑漏洞的知识体系吧。适合刚入门渗透的童鞋看

十分钟看完，全书没有一点诚意，完全是为了出书而出书。全书讲了80%的burp怎么用，20%讲怎么重复提交，100%讲的是废话。如果满分是100分的话，我愿意给个负分，当时离开这个圈子是觉得这个圈子太浮躁，近几年有很多安全的书出版，我还以为氛围变了呢，现在原来是个人就能出书啦 了不起啊

感觉不到作者的诚意,测试环境都没有提供。。。

这本书就是个坑。像过家家一样，就这样还好意思出书，浪费了我50块钱。余弦也是个坑B，蛇鼠一窝。这本书其实就目录有用，内容。。呵呵。

半个小时就看完的书 很没意思 我也能写一本
玩渗透又没有实战经验的人可以看看电子版 偶然看到别人买的看完没学到一点新东西
非常没有诚意的一本书 简直就是“十天速成黑客”的进化版

[Web攻防之业务安全实战指南_下载链接1](#)

书评

感觉不到作者的诚意啊,连个测试环境作者都不给出,实在是太不厚道了..建议这种书籍只需要看看电子版的即可。。。没有必要买字纸版的,真是的是浪费金钱啊.如果满分是100分的话，我愿意给个不及格,国内人大多数感觉只是为了出书而出书。。。想学习真正的知识还是转到国外吧,比如h1...

[Web攻防之业务安全实战指南 下载链接1](#)