

Web应用安全权威指南



[Web应用安全权威指南_下载链接1_](#)

著者:德丸浩

出版者:人民邮电出版社

出版时间:2014-10

装帧:平装

isbn:9787115370471

《web应用安全权威指南》系日本web安全第一人德丸浩所创，是作者从业多年的经验总结。作者首先简要介绍了web应用的安全隐患以及产生原因，然后详细介绍了web安全的基础，如http、会话管理、同源策略等。此外还重点介绍了web应用的各种安全隐患，对其产生原理及对策进行了详尽的讲解。最后对如何提高web网站的安全性和开发

安全的web应用所需要的管理进行了深入的探讨。本书可操作性强，读者可以通过下载已搭建的虚拟机环境亲身体验书中的各种安全隐患。

《web应用安全权威指南》适合web相关的开发人员特别是安全及测试人员阅读。

八大章节全面剖析，深入浅出地讲解了sql注入、xss、csrf等web开发人员必知的web安全知识。通过在vmware player虚拟机上对php样本的攻击，详细介绍了安全隐患产生的原理及应对方法，助你打造安全无虞的web应用。

作者介绍:

德丸 浩

2008年创立HASH咨询公司，任董事长。主要从事网络安全性的诊断与咨询工作，并在工作之余通过博客普及网络安全知识。兼任KYOCERA Communication Systems股份有限公司技术顾问、独立行政法人信息处理推进机构（IPA）兼职研究员。Twitter ID为@ockeghem。

赵文

程序员，Ruby 语言爱好者。图灵电子书《关于 mruby 的一切》译者。个人博客：<http://zhaowen.me>

刘斌

程序员，关注于后台开发，Java/Ruby爱好者。个人主页：<http://liubin.org>

目录: 第1章 什么是 web应用的安全隐患 1

1-1 安全隐患即“能用于作恶的bug” 2

1-2 为什么存在安全隐患会有问题 3

经济损失 3

法律要求 3

对用户造成不可逆的伤害 4

欺骗用户 4

被用于构建僵尸网络 4

1-3 产生安全隐患的原因 6

1-4 安全性 bug与安全性功能 7

1-5 本书的结构 8

第2章 搭建试验环境 9

2-1 试验环境概要 10

2-2 安装 vmware player 11

什么是 vmware player 11

下载 vmware player 11

安装 vmware player 12

2-3 安装虚拟机及运行确认 14

虚拟机启动确认 14

虚拟机的使用方法 15

编辑 hosts文件 16

使用 ping确认连接 16

apache 与php的运行确认 17

设置并确认邮箱账号 17

2-4 安装 fiddler 18
什么是 fiddler 18
安装 fiddler 18
fiddler 的运行确认及简单用法 18
参考：虚拟机的数据一览 19
参考：如果无法连接试验环境的pop3服务器 20
第3章 web 安全基础：http、会话管理、同源策略 21
3-1 http 与会话管理 22
为什么要学习 http 22
最简单的 http 22
使用 fiddler观察http消息 23
请求消息 24
响应消息 24
状态行 25
响应头信息 25
如果将 http比喻为对话 25
输入—确认—注册模式 26
post 方法 28
消息体 28
百分号编码 29
referer 29
get 和post的使用区别 29
hidden 参数能够被更改 30
将 hidden参数的更改比作对话 32
hidden 参数的优点 32
无状态的 http认证 33
体验 basic认证 33
专栏 认证与授权 36
cookie 与会话管理 36
使用 cookie的会话管理 39
会话管理的拟人化解说 39
会话 id泄漏的原因 42
cookie 的属性 42
专栏 cookie monster bug 44
总结 45
3-2 被动攻击与同源策略 46
主动攻击与被动攻击 46
主动攻击 46
被动攻击 46
恶意利用正规网站进行的被动攻击 47
跨站被动攻击 48
浏览器如何防御被动攻击 48
沙盒 49
同源策略 49
应用程序安全隐患与被动攻击 52
专栏 第三方 javascript 53
javascript 以外的跨域访问 54
frame 元素与iframe元素 54
专栏 x-frame-options 54
img 元素 54
script 元素 54
css 55
form 元素的action属性 55
总结 56

- 第4章 web应用的各种安全隐患 57
 - 4-1 web 应用的功能与安全隐患的对应关系 58
 - 安全隐患产生于何处 58
 - 注入型隐患 59
 - 总结 60
 - 4-2 输入处理与安全性 61
 - 什么是 web应用的输入处理 61
 - 检验字符编码 62
 - 转换字符编码 62
 - 检验并转换字符编码的实例 62
 - 专栏 字符编码的自动转换与安全性 64
 - 输入校验 64
 - 输入校验的目的 64
 - 输入校验与安全性 65
 - 二进制安全与空字节攻击 65
 - 仅校验输入值并不是安全性策略 66
 - 输入校验的依据是应用程序的规格 67
 - 哪些参数需要校验 67
 - php 的正则表达式库 67
 - 使用正则表达式检验输入值的实例 (1) 1~5 个字符的字母数字 68
 - 使用正则表达式检验输入值的实例 (2) 住址栏 70
 - 专栏 请注意 mb_ereg中的\d与\w 70
 - 范例 70
 - 专栏 输入校验与框架 71
 - 总结 72
 - 参考：表示“非控制字符的字符”的正则表达式 73
 - 4-3 页面显示的相关问题 75
 - 4.3.1 跨站脚本（基础篇） 75
 - 概要 75
 - 攻击手段与影响 76
 - xss 窃取cookie值 76
 - 通过 javascript攻击 79
 - 篡改网页 80
 - 反射型 xss与存储型xss 82
 - 安全隐患的产生原因 84
 - html 转义的概要 84
 - 元素内容的 xss 85
 - 没有用引号括起来的属性值的 xss 85
 - 用引号括起来的属性值的 xss 85
 - 对策 86
 - xss 对策的基础 86
 - 指定响应的字符编码 87
 - xss 的辅助性对策 88
 - 对策总结 89
 - 参考：使用perl的对策示例 89
 - 使用 perl进行html转义的方法 89
 - 指定响应的字符编码 89
 - 4.3.2 跨站脚本（进阶篇） 90
 - href 属性与src属性的xss 91
 - 生成 url时的对策. 92
 - 校验链接网址 92
 - javascript 的动态生成 92
 - 事件绑定函数的 xss 92
 - script 元素的xss 94

- javascript 字符串字面量动态生成的对策 95
- dom based xss 97
- 允许 html 标签或 css 时的对策 99
- 参考：perl 中转义 unicode 的函数 99
- 4.3.3 错误消息导致的信息泄漏 100
- 总结 100
- 继续深入学习 100
- 4-4 sql 调用相关的安全隐患 101
- 4.4.1 sql 注入 101
- 概要 101
- 攻击手段与影响 102
- 示例脚本解说 102
- 错误消息导致的信息泄漏 103
- union select 致使的信息泄漏 104
- 使用 sql 注入绕过认证 104
- 通过 sql 注入攻击篡改数据 106
- 其他攻击 107
- 专栏 数据库中表名与列名的调查方法 108
- 安全隐患的产生原因 109
- 字符串字面量的问题 109
- 针对数值的 sql 注入攻击 110
- 对策 110
- 使用占位符拼接 sql 语句 111
- 专栏 采用 mdb2 的原因 111
- 为什么使用占位符会安全 111
- 参考：like 语句与通配符 113
- 使用占位符的各种处理 114
- sql 注入的辅助性对策 116
- 总结 117
- 继续深入学习 117
- 参考：无法使用占位符时的对策 117
- 参考：perl+mysql 的安全连接方法 118
- 参考：php+pdo+mysql 的安全连接方法 118
- 参考：java+mysql 的安全连接方法 118
- 4-5 关键处理中引入的安全隐患 120
- 4.5.1 跨站请求伪造 (csrf) 120
- 概要 120
- 攻击手段与影响 121
- 输入—执行”模式的 csrf 攻击 121
- csrf 攻击与 xss 攻击 124
- 存在确认页面时的 csrf 攻击 125
- 专栏 针对内部网络的 csrf 攻击 127
- 安全隐患的产生原因 128
- 对策 129
- 筛选出需要防范 csrf 攻击的页面 129
- 确认是正规用户自愿发送的请求 130
- 专栏 令牌与一次性令牌 131
- csrf 的辅助性对策 133
- 对策总结 133
- 4-6 不完善的会话管理 134
- 4.6.1 会话劫持的原因及影响 134
- 预测会话 id 134
- 窃取会话 id 134
- 挟持会话 id 135

- 会话劫持的方法总结 135
- 会话劫持的影响 135
- 4.6.2 会话 id 可预测 136
 - 概要 136
 - 攻击手段与影响 136
 - 常见的会话 id 生成方法 136
 - 使用推测出的会话 id 尝试伪装 137
 - 伪装造成的影响 137
 - 安全隐患的产生原因 137
 - 对策 138
 - 改善 php 的会话 id 的随机性的方法 138
 - 参考：自制会话管理机制产生的其他隐患 139
- 4.6.3 会话 id 嵌入 url 139
 - 概要 139
 - 攻击手段与影响 140
 - 会话 id 嵌入 url 所需的条件 140
 - 范例脚本解说 141
 - 通过 referer 泄漏会话 id 所需的条件 142
 - 攻击流程 142
 - 事故性的会话 id 泄漏 143
 - 影响 144
 - 安全隐患的产生原因 144
 - 对策 144
 - php 144
 - java servlet (j2ee) 145
 - asp.net 145
- 4.6.4 固定会话 id 145
 - 概要 145
 - 攻击手段与影响 146
 - 示例脚本介绍 146
 - 会话固定攻击解说 148
 - 登录前的会话固定攻击 148
 - 会话采纳 151
 - 仅在 cookie 中保存会话 id 的网站固定会话 id 151
 - 会话固定攻击的影响 151
 - 安全隐患的产生原因 152
 - 对策 152
 - 无法更改会话 id 时采用令牌 153
 - 登录前的会话固定攻击的对策 154
 - 总结 154
- 4-7 重定向相关的安全隐患 155
 - 4.7.1 自由重定向漏洞 155
 - 概要 155
 - 攻击手段与影响 156
 - 安全隐患的产生原因 159
 - 允许自由重定向的情况 159
 - 对策 160
 - 固定重定向的目标 url 160
 - 使用编号指定重定向的目标 url 160
 - 校验重定向的目标域名 160
 - 专栏 警告页面 162
 - 4.7.2 http 消息头注入 162
 - 概要 162
 - 攻击手段与影响 163

- 重定向至外部域名 165
- 专栏 http 响应截断攻击 166
- 生成任意 cookie 166
- 显示伪造页面 168
- 安全隐患的产生原因 170
- 专栏 http 消息头与换行 171
- 对策 171
- 对策 1: 不将外界参数作为http响应消息头输出 171
- 对策 2: 执行以下两项内容 171
- 专栏 php 的header函数中进行的换行符校验 173
- 4.7.3 重定向相关的安全隐患总结 173
- 4-8 cookie 输出相关的安全隐患 174
- 4.8.1 cookie 的用途不当 174
- 不该保存在 cookie 中的数据 174
- 参考: 最好不要在cookie中保存数据的原因 174
- 专栏 padding oracle 攻击与ms10-070 176
- 4.8.2 cookie 的安全属性设置不完善 176
- 概要 176
- 攻击手段与影响 177
- 关于抓包方法的注意点 180
- 安全隐患的产生原因 181
- 什么样的应用程序不能在 cookie 中设置安全属性 181
- 对策 181
- 给保存会话 id 的 cookie 设置安全属性的方法 182
- 使用令牌的对策 182
- 使用令牌能确保安全性的原因 184
- 除安全属性外其他属性值需要注意的地方 184
- domain 属性 184
- path 属性 185
- expires 属性 185
- httponly 属性 185
- 总结 185
- 4-9 发送邮件的问题 186
- 4.9.1 发送邮件的问题概要 186
- 邮件头注入漏洞 186
- 使用 hidden 参数保存收件人信息 186
- 参考: 邮件服务器的开放转发 187
- 4.9.2 邮件头注入漏洞 187
- 概要 187
- 攻击手段与影响 188
- 攻击方式 1: 添加收件人 190
- 攻击方式 2: 篡改正文 191
- 通过邮件头注入攻击添加附件 192
- 安全隐患的产生原因 193
- 对策 194
- 使用专门的程序库来发送邮件 194
- 不将外界传入的参数包含在邮件头中 194
- 发送邮件时确保外界传入的参数中不包含换行符 195
- 邮件头注入的辅助性对策 195
- 总结 196
- 继续深入学习 196
- 10-4 文件处理相关的问题 197
- 4.10.1 目录遍历漏洞 197
- 概要 197

- 攻击手段与影响 198
- 专栏 从脚本源码开始的一连串的信息泄漏 200
- 安全隐患的产生原因 200
- 对策 201
- 避免由外界指定文件名 201
- 文件名中不允许包含目录名 201
- 专栏 basename 函数与空字节 202
- 限定文件名中仅包含字母和数字 202
- 总结 203
- 4.10.2 内部文件被公开 203
- 概要 203
- 攻击手段与影响 203
- 安全隐患的产生原因 204
- 对策 205
- 参考：apache中隐藏特定文件的方法 205
- 11-4 调用 os命令引起的安全隐患 206
- 4.11.1 os 命令注入 206
- 概要 206
- 攻击手段与影响 207
- 调用 sendmail命令发送邮件 207
- os 命令注入攻击与影响 209
- 安全隐患的产生原因 210
- 在 shell中执行多条命令 210
- 使用了内部调用 shell的函数 211
- 安全隐患的产生原因总结 212
- 对策 212
- 在设计阶段决定对策方针 213
- 选择不调用 os命令的实现方法 213
- 避免使用内部调用 shell的函数 213
- 不将外界输入的字符串传递给命令行参数 216
- 使用安全的函数对传递给 os命令的参数进行转义 216
- os 命令注入攻击的辅助性对策 217
- 参考：内部调用shell的函数 218
- 12-4 文件上传相关的问题 219
- 4.12.1 文件上传问题的概要 219
- 针对上传功能的 dos攻击 219
- 专栏 内存使用量与 cpu使用时间等其他需要关注的资源 220
- 使上传的文件在服务器上作为脚本执行 220
- 诱使用户下载恶意文件 221
- 越权下载文件 222
- 4.12.2 通过上传文件使服务器执行脚本 222
- 概要 222
- 攻击手段与影响 223
- 示例脚本解说 223
- 专栏 警惕文件名中的 xss 224
- php 脚本的上传与执行 224
- 安全隐患的产生原因 225
- 对策 225
- 专栏 校验扩展名时的注意点 228
- 4.12.3 文件下载引起的跨站脚本 228
- 概要 228
- 攻击手段与影响 229
- 图像文件引起的 xss 229
- pdf 下载引起的xss 231

- 安全隐患的产生原因 234
 - 内容为图像时 234
 - 内容不为图像时 235
- 对策 236
 - 文件上传时的对策 236
- 专栏 bmp 格式的注意点与ms07-057 238
- 文件下载时的对策 238
- 其他对策 239
 - 专栏 将图像托管在其他域名 240
- 参考：用户pc中没有安装对应的应用程序时 240
- 总结 241
- 13-4 include 相关的问题 242
 - 4.13.1 文件包含攻击 242
- 概要 242
- 攻击手段与影响 243
- 文件包含引发的信息泄漏 244
- 执行脚本 1：远程文件包含攻击（rfi） 244
 - 专栏 rfi 攻击的变种 245
- 执行脚本 2：恶意使用保存会话信息的文件 246
- 安全隐患的产生原因 248
 - 对策 248
- 总结 248
- 14-4 eval 相关的问题 249
 - 4.14.1 eval 注入 249
- 概要 249
- 攻击手段与影响 250
- 存在漏洞的应用 250
- 攻击手段 252
- 安全隐患的产生原因 253
 - 对策 253
- 不使用 eval 253
- 避免 eval的参数中包含外界传入的参数 254
- 限制外界传入 eval的参数中只包含字母和数字 254
- 参考：perl的eval代码块形式 254
- 总结 255
- 继续深入学习 255
- 15-4 共享资源相关的问题 256
 - 4.15.1 竞态条件漏洞 256
- 概要 256
- 攻击手段与影响 257
- 安全隐患的产生原因 258
 - 对策 259
- 避免使用共享资源 259
- 使用互斥锁 259
- 总结 260
- 参考：java servlet的其他注意点 260

第5章 典型安全功能 261

5-1 认证 262

5.1.1 登录功能 262

- 针对登录功能的攻击 262
 - 通过 sql注入攻击来跳过登录功能 262
 - 通过 sql注入攻击获取用户密码 263
 - 在登录页面进行暴力破解 263
 - 通过社会化攻击得到用户密码 263

- 通过钓鱼方法获取密码 264
- 登录功能被破解后的影响 264
- 如何防止非法登录 264
- 确保系统中不存在 sql注入等安全性bug 264
- 设置难以猜测的密码 265
- 密码的字符种类和长度要求 265
- 密码的使用现状 266
- 应用程序设计中关于密码的需求 266
- 严格的密码检查原则 267
- 5.1.2 针对暴力破解攻击的对策 268
 - 初步认识账号锁定 268
 - 暴力破解攻击的检测和对策 268
 - 字典攻击 269
 - joe 账号检索 269
 - 逆向暴力破解 269
 - 针对变种暴力破解的对策 269
- 5.1.3 密码保存方法 271
 - 保护密码的必要性 271
 - 利用加密方式进行密码保护及其注意事项 271
 - 专栏 数据库加密和密码保护 272
 - 利用信息摘要来进行密码保护及其注意事项 272
 - 什么是信息摘要 272
 - 专栏 密码学级别的散列函数需要满足的要求 273
 - 利用信息摘要保护密码 273
 - 威胁 1: 离线暴力破解 274
 - 威胁 2: 彩虹破解 (rainbow crack) 275
 - 威胁 3: 在用户数据库里创建密码字典 276
 - 如何防止散列值被破解 277
 - 对策 1: salt (加盐) 277
 - 对策 2: stretching (延展计算) 278
 - 实现示例 278
 - 专栏 密码泄露途径 280
- 5.1.4 自动登录 280
 - 危险的实现方式示例 281
 - 安全的自动登录实现方式 281
 - 延长会话有效期 282
 - 使用令牌实现自动登录 283
 - 基于认证票的自动登录方式 286
 - 三种方法的比较 286
 - 如何降低自动登录带来的风险 286
- 5.1.5 登录表单 286
 - 专栏 密码确实需要掩码显示吗 287
- 5.1.6 如何显示错误消息 288
- 5.1.7 退出登录功能 289
- 5.1.8 认证功能总结 290
- 参考: 彩虹表原理 290
- 5-2账号管理 293
 - 5.2.1 用户注册 293
 - 邮箱地址确认 293
 - 防止用户 id重复 295
 - 例子 1: id相同密码不同可以注册的网站 295
 - 例子 2: 用户id没有添加唯一性约束的网站 295
 - 应对自动用户注册 296
 - 利用 captcha防止自动注册 296

- 5.2.2 修改密码 297
- 确认当前密码 297
- 修改密码后向用户发送邮件通知 298
- 密码修改功能容易发生的漏洞 298
- 5.2.3 修改邮箱地址 298
- 修改邮箱地址功能要考虑的安全对策 299
- 5.2.4 密码找回 299
- 面向管理员的密码找回功能 300
- 面向用户的密码找回功能 300
- 对用户进行身份确认 301
- 如何发送密码通知 301
- 5.2.5 账号冻结 302
- 5.2.6 账号删除 303
- 5.2.7 账号管理总结 303
- 5.3 授权 304
- 5.3.1 什么是授权 304
- 5.3.2 典型的授权漏洞 304
- 更改资源 id后可以查看没有权限查看的信息 304
- 只控制菜单的显示或不显示 305
- 使用 hidden参数或者cookie保存权限信息 306
- 授权漏洞总结 307
- 专栏 将私密信息嵌入 url进行授权处理 307
- 5.3.3 授权管理的需求设计 307
- 专栏 什么是角色 308
- 5.3.4 如何正确实现授权管理 308
- 5.3.5 总结 309
- 5.4 日志输出 310
- 5.4.1 日志输出的目的 310
- 5.4.2 日志种类 310
- 错误日志 311
- 访问日志 311
- 调试日志 311
- 5.4.3 有关日志输出的需求 311
- 需要记录到日志里的所有事件 312
- 日志里应包括的信息和格式 312
- 日志文件保护 312
- 日志文件保存位置 313
- 日志文件保存期限 313
- 服务器的时间调整 313
- 5.4.4 实现日志输出 313
- 5.4.5 总结 314
- 第6章 字符编码和安全 315
- 6-1 字符编码和安全概要 316
- 6-2 字符集 317
- 什么是字符集 317
- ascii 和iso-8859-1 317
- jis 规定的字符集 318
- 微软标准字符集 318
- unicode 319
- gb2312 319
- gbk 319
- gb18030 320
- 不同字符相同编码的问题 320
- 字符集的处理引起的漏洞 320

- 6-3 字符编码方式 321
 - 什么是编码方式 321
 - shift_jis 321
 - euc-jp 325
 - iso-2022-jp 326
 - utf-16 326
 - utf-8 327
 - gb2312 329
 - gbk 330
 - gb18030 331
- 6-4 由字符编码引起的漏洞总结 332
 - 字符编码方式中非法数据导致的漏洞 332
 - 对字符编码方式处理存在纰漏导致的漏洞 332
 - 在不同字符集间变换导致的漏洞 332
- 6-5 如何正确处理字符编码 333
 - 在应用内统一使用的字符集 333
 - 输入非法数据时报错并终止处理 335
 - 处理数据时使用正确的编码方式 335
 - 专栏 调用 htmlspecialchars 函数时必须指定字符编码方式 336
 - 输出时设置正确的字符编码方式 336
 - 其他对策：尽量避免编码自动检测 337
- 6-6 总结 338
- 如何提高 web 网站的安全性 第7章 339
 - 7-1 针对 web 服务器的攻击途径和防范措施 341
 - 7.1.1 利用基础软件漏洞进行攻击 341
 - 7.1.2 非法登录 341
 - 7.1.3 对策 341
 - 停止运行不需要的软件 342
 - 定期实施漏洞防范措施 342
 - 选定软件时确认软件的升级状况 342
 - 确定打补丁方式 343
 - 关注各种漏洞相关信息 344
 - 确认漏洞后调查补丁状况以及防范对策、并制定对应计划 344
 - 执行漏洞对应计划 345
 - 对不需要对外公开的端口或服务加以访问限制 346
 - 通过端口扫描确认各端口服务状态 347
 - 提高认证强度 348
- 7-2 防范伪装攻击的对策 349
 - 7.2.1 网络伪装的手段 349
 - 针对 dns 服务器的攻击 349
 - 专栏 visa 域名问题 350
 - arp 欺骗攻击 350
 - 7.2.2 钓鱼攻击 350
 - 7.2.3 web 网站的伪装攻击对策 351
- 网络层的对策 351
 - 同一网段内不放置可能存在漏洞的服务器 351
 - 强化 dns 运维 351
 - 引入 ssl/tls 352
 - 专栏 免费的数字证书 354
 - 使用便于记忆的域名 354
- 7-3 防范网络监听、篡改的对策 355
 - 7.3.1 网络监听、篡改的途径 355
 - 通过无线网进行监听、篡改 355
 - 利用交换机端口镜像 355

利用代理服务器 355
伪装成 dhcp服务器 355
使用 arp欺骗攻击和dns缓存污染攻击 (dns cache poisoning) 355
7.3.2 中间人攻击 356
使用 fiddler模拟中间人攻击 356
专栏 请不要手动安装证书 358
7.3.3 对策 359
使用 ssl时的注意事项 359
专栏 ssl 认证标签 360
7-4 防范恶意软件的对策 361
7.4.1 什么是 web网站的恶意软件对策 361
7.4.2 恶意软件的感染途径 361
7.4.3 web 网站恶意软件防范对策概要 362
7.4.4 如何确保服务器不被恶意软件感染 363
探讨是否需要制定针对恶意软件的防范措施 363
制定病毒防范政策并向用户公开 363
使用防病毒软件 364
专栏 web 网站的防病毒对策和gumblar的关系 365
7-5 总结 366
开发安全的 web应用所需要的管理 第8章 367
8-1 开发管理中的安全对策概要 368
8-2 开发体制 369
开发标准的制定 369
教育培训 369
8-3 开发过程 371
8.3.1 规划阶段的注意事项 371
8.3.2 招标时的注意事项 371
专栏 谁应该对安全漏洞负责 372
8.3.3 需求分析时的注意事项 372
8.3.4 概要设计的推进方法 373
8.3.5 详细设计和编码阶段的注意事项 374
8.3.6 安全性测试的重要性及其方法 374
8.3.7 web 健康诊断基准 374
8.3.8 承包方测试 376
8.3.9 发包方测试 (验收) 376
8.3.10 运维阶段的注意事项 377
8-4 总结 378
• • • • • (收起)

[Web应用安全权威指南_下载链接1](#)

标签

安全

web安全

信息安全

Web

计算机

软件开发

互联网

网络安全

评论

挺好的

web安全最佳入门。

比较实用，不过暂时没用上。

这么好的书.....

好书，得再翻几遍;从“除了自己，谁都不可信”发展到“自己都不可信”。

针对初学者的安全用书，适合大众科普……

首先肯定是本很好的入门书，然后才是好啰嗦啊。

非常全面，脉络清晰，收获很大

大部分内容还是太过基础了，开发过程中稍微注意一些都可以避免。唯一的收获就是作为用户对XSS漏洞的危害有了更深的认识

PHP实例，但是可以上手体验，内容很丰富，讲解地很浅显易懂。
总之非常不错书籍，之前虽然有过一点web开发经验，但是在安全方面基本一片空白读了大有裨益。(竟然是放假回家发现我堂弟买的。。才拿来读

很全面，但是比较零碎繁杂、不深入。

日本师傅的工匠精神可谓有以致之，本书非常全面，把web安全的框架都展开来讲得很清楚了 缺点嘛，太厚，做笔记的话，效率就高不起来。
不过管他的，最重要的是学东西嘛 读完了，不错

第三、五、六章可读

入门级。对整体有一个系统的了解，讲到的点都讲的很清楚。

内容很广，各方面都有涉及，和《黑客攻防技术宝典Web实战篇》有些类似，两个看一本就够了，这本书在防护方面讲的更多一些。

日本同行中规中矩 没有太多故事讲 字字都为主题服务。略显不够的是 例子太单调了 不能饱满地勾勒出攻击和防御的画面。源码不知为何一定携带一个虚拟机

地址是：<http://www.ituring.com.cn/book/download/d2970acc-5c0f-45ae-857d-be55a5421be4>

这书也是别人推荐来读的，当时也的确被封面上的‘在虚拟机上体验攻击流程’吸引了。读完一遍后的感受是，这本书的确是偏防御的，涵盖的面比较广，对于每种安全问题都给了应对策略，不过所谓的‘攻击流程’这个就有点言过其实了，无非就是给几段有安全漏洞的php代码，然后进入存在该恶意代码的网站体验下后果(该网站的服务器位于虚拟机中)然后分析下就完事了，没有让我感受到那种实战的快感

内容比较浅显，易懂，而且非常详实，解释的概念很清楚，例子很形象。非常适合初中级开发人员，尤其是对安全问题一知半解的工程师。

[Web应用安全权威指南 下载链接1](#)

书评

这是一本对 web 安全讲解的非常全面的一本书，虽然可能没有国内道哥和余弦那两本书的深度，没讲什么攻击的奇淫技巧，但是有那两本书的广度，感觉这本更偏重防，当做指南还是不错的，对各种 web 应用安全的防范策略介绍的非常全面，每个 web 开发者都应该去读读。

[Web应用安全权威指南 下载链接1](#)