

# 白帽子讲Web安全



[白帽子讲Web安全\\_下载链接1](#)

著者:吴翰清

出版者:电子工业出版社

出版时间:2012-3

装帧:平装

isbn:9787121160721

《白帽子讲Web安全》内容简介：在互联网时代，数据安全与个人隐私受到了前所未有的

的挑战，各种新奇的攻击技术层出不穷。如何才能更好地保护我们的数据？《白帽子讲Web安全》将带你走进Web安全的世界，让你了解Web安全的方方面面。黑客不再变得神秘，攻击技术原来我也可以会，小网站主自己也能找到正确的安全道路。大公司是怎么做安全的，为什么要选择这样的方案呢？你能在《白帽子讲Web安全》中找到答案。详细的剖析，让你不仅能“知其然”，更能“知其所以然”。

作者介绍:

吴翰清，毕业于西安交通大学少年班，从2000年开始研究网络攻防技术。在大学期间创立了在中国安全圈内极具影响力的组织“幻影”。

目录: 第一篇 世界观安全

第1章 我的安全世界观 2

1.1 Web安全简史 2

1.1.1 中国黑客简史 2

1.1.2 黑客技术的发展历程 3

1.1.3 Web安全的兴起 5

1.2 黑帽子，白帽子 6

1.3 返璞归真，揭秘安全的本质 7

1.4 破除迷信，没有银弹 9

1.5 安全三要素 10

1.6 如何实施安全评估 11

1.6.1 资产等级划分 12

1.6.2 威胁分析 13

1.6.3 风险分析 14

1.6.4 设计安全方案 15

1.7 白帽子兵法 16

1.7.1 Secure By Default原则 16

1.7.2 纵深防御原则 18

1.7.3 数据与代码分离原则 19

1.7.4 不可预测性原则 21

1.8 小结 22

(附) 谁来为漏洞买单? 23

第二篇 客户端脚本安全

第2章 浏览器安全 26

2.1 同源策略 26

2.2 浏览器沙箱 30

2.3 恶意网址拦截 33

2.4 高速发展的浏览器安全 36

2.5 小结 39

第3章 跨站脚本攻击 (XSS) 40

3.1 XSS简介 40

3.2 XSS攻击进阶 43

3.2.1 初探XSS Payload 43

3.2.2 强大的XSS Payload 46

3.2.3 XSS 攻击平台 62

3.2.4 终极武器: XSS Worm 64

3.2.5 调试JavaScript 73

3.2.6 XSS构造技巧 76

3.2.7 变废为宝: Mission Impossible 82

3.2.8 容易被忽视的角落: Flash XSS 85

3.2.9 真的高枕无忧吗: JavaScript开发框架 87

- 3.3 XSS的防御 89
  - 3.3.1 四两拨千斤：HttpOnly 89
  - 3.3.2 输入检查 93
  - 3.3.3 输出检查 95
  - 3.3.4 正确地防御XSS 99
  - 3.3.5 处理富文本 102
  - 3.3.6 防御DOM Based XSS 103
  - 3.3.7 换个角度看XSS的风险 107
- 3.4 小结 107
- 第4章 跨站点请求伪造（CSRF） 109
  - 4.1 CSRF简介 109
  - 4.2 CSRF进阶 111
    - 4.2.1 浏览器的Cookie策略 111
    - 4.2.2 P3P头的副作用 113
    - 4.2.3 GET? POST? 116
    - 4.2.4 Flash CSRF 118
    - 4.2.5 CSRF Worm 119
  - 4.3 CSRF的防御 120
    - 4.3.1 验证码 120
    - 4.3.2 Referer Check 120
    - 4.3.3 Anti CSRF Token 121
  - 4.4 小结 124
- 第5章 点击劫持（ClickJacking） 125
  - 5.1 什么是点击劫持 125
  - 5.2 Flash点击劫持 127
  - 5.3 图片覆盖攻击 129
  - 5.4 拖拽劫持与数据窃取 131
  - 5.5 ClickJacking 3.0：触屏劫持 134
  - 5.6 防御ClickJacking 136
    - 5.6.1 frame busting 136
    - 5.6.2 X-Frame-Options 137
  - 5.7 小结 138
- 第6章 HTML 5 安全 139
  - 6.1 HTML 5新标签 139
    - 6.1.1 新标签的XSS 139
    - 6.1.2 iframe的sandbox 140
    - 6.1.3 Link Types: norereferrer 141
    - 6.1.4 Canvas的妙用 141
  - 6.2 其他安全问题 144
    - 6.2.1 Cross-Origin Resource Sharing 144
    - 6.2.2 postMessage——跨窗口传递消息 146
    - 6.2.3 Web Storage 147
  - 6.3 小结 150
- 第三篇 服务器端应用安全
- 第7章 注入攻击 152
  - 7.1 SQL注入 152
    - 7.1.1 盲注（Blind Injection） 153
    - 7.1.2 Timing Attack 155
  - 7.2 数据库攻击技巧 157
    - 7.2.1 常见的攻击技巧 157
    - 7.2.2 命令执行 158
    - 7.2.3 攻击存储过程 164
    - 7.2.4 编码问题 165
    - 7.2.5 SQL Column Truncation 167

7.3 正确地防御SQL注入	170
7.3.1 使用预编译语句	171
7.3.2 使用存储过程	172
7.3.3 检查数据类型	172
7.3.4 使用安全函数	172
7.4 其他注入攻击	173
7.4.1 XML注入	173
7.4.2 代码注入	174
7.4.3 CRLF注入	176
7.5 小结	179
第8章 文件上传漏洞	180
8.1 文件上传漏洞概述	180
8.1.1 从FCKEditor文件上传漏洞谈起	181
8.1.2 绕过文件上传检查功能	182
8.2 功能还是漏洞	183
8.2.1 Apache文件解析问题	184
8.2.2 IIS文件解析问题	185
8.2.3 PHP CGI路径解析问题	187
8.2.4 利用上传文件钓鱼	189
8.3 设计安全的文件上传功能	190
8.4 小结	191
第9章 认证与会话管理	192
9.1 Who am I?	192
9.2 密码的那些事儿	193
9.3 多因素认证	195
9.4 Session与认证	196
9.5 Session Fixation攻击	198
9.6 Session保持攻击	199
9.7 单点登录 (SSO)	201
9.8 小结	203
第10章 访问控制	205
10.1 What Can I Do?	205
10.2 垂直权限管理	208
10.3 水平权限管理	211
10.4 OAuth简介	213
10.5 小结	219
第11章 加密算法与随机数	220
11.1 概述	220
11.2 Stream Cipher Attack	222
11.2.1 Reused Key Attack	222
11.2.2 Bit-flipping Attack	228
11.2.3 弱随机IV问题	230
11.3 WEP破解	232
11.4 ECB模式的缺陷	236
11.5 Padding Oracle Attack	239
11.6 密钥管理	251
11.7 伪随机数问题	253
11.7.1 弱伪随机数的麻烦	253
11.7.2 时间真的随机吗	256
11.7.3 破解伪随机数算法的种子	257
11.7.4 使用安全的随机数	265
11.8 小结	265
(附) Understanding MD5 Length Extension Attack	267
第12章 Web框架安全	280

- 12.1 MVC框架安全 280
- 12.2 模板引擎与XSS防御 282
- 12.3 Web框架与CSRF防御 285
- 12.4 HTTP Headers管理 287
- 12.5 数据持久层与SQL注入 288
- 12.6 还能想到什么 289
- 12.7 Web框架自身安全 289
  - 12.7.1 Struts 2命令执行漏洞 290
  - 12.7.2 Struts 2的问题补丁 291
  - 12.7.3 Spring MVC命令执行漏洞 292
  - 12.7.4 Django命令执行漏洞 293
- 12.8 小结 294
- 第13章 应用层拒绝服务攻击 295
  - 13.1 DDOS简介 295
  - 13.2 应用层DDOS 297
    - 13.2.1 CC攻击 297
    - 13.2.2 限制请求频率 298
    - 13.2.3 道高一尺，魔高一丈 300
  - 13.3 验证码的那些事儿 301
  - 13.4 防御应用层DDOS 304
  - 13.5 资源耗尽攻击 306
    - 13.5.1 Slowloris攻击 306
    - 13.5.2 HTTP POST DOS 309
    - 13.5.3 Server Limit DOS 310
  - 13.6 一个正则引发的血案：ReDOS 311
  - 13.7 小结 315
- 第14章 PHP安全 317
  - 14.1 文件包含漏洞 317
    - 14.1.1 本地文件包含 319
    - 14.1.2 远程文件包含 323
    - 14.1.3 本地文件包含的利用技巧 323
  - 14.2 变量覆盖漏洞 331
    - 14.2.1 全局变量覆盖 331
    - 14.2.2 extract()变量覆盖 334
    - 14.2.3 遍历初始化变量 334
    - 14.2.4 import\_request\_variables变量覆盖 335
    - 14.2.5 parse\_str()变量覆盖 335
  - 14.3 代码执行漏洞 336
    - 14.3.1 “危险函数”执行代码 336
    - 14.3.2 “文件写入”执行代码 343
    - 14.3.3 其他执行代码方式 344
  - 14.4 定制安全的PHP环境 348
  - 14.5 小结 352
- 第15章 Web Server配置安全 353
  - 15.1 Apache安全 353
  - 15.2 Nginx安全 354
  - 15.3 jBoss远程命令执行 356
  - 15.4 Tomcat远程命令执行 360
  - 15.5 HTTP Parameter Pollution 363
  - 15.6 小结 364
- 第四篇 互联网公司安全运营
- 第16章 互联网业务安全 366
  - 16.1 产品需要什么样的安全 366
    - 16.1.1 互联网产品对安全的需求 367

16.1.2 什么是好的安全方案	368
16.2 业务逻辑安全	370
16.2.1 永远改不掉的密码	370
16.2.2 谁是大赢家	371
16.2.3 瞒天过海	372
16.2.4 关于密码取回流程	373
16.3 账户是如何被盗的	374
16.3.1 账户被盗的途径	374
16.3.2 分析账户被盗的原因	376
16.4 互联网的垃圾	377
16.4.1 垃圾的危害	377
16.4.2 垃圾处理	379
16.5 关于网络钓鱼	380
16.5.1 钓鱼网站简介	381
16.5.2 邮件钓鱼	383
16.5.3 钓鱼网站的防控	385
16.5.4 网购流程钓鱼	388
16.6 用户隐私保护	393
16.6.1 互联网的用户隐私挑战	393
16.6.2 如何保护用户隐私	394
16.6.3 Do-Not-Track	396
16.7 小结	397
(附) 麻烦的终结者	398
第17章 安全开发流程 (SDL)	402
17.1 SDL简介	402
17.2 敏捷SDL	406
17.3 SDL实战经验	407
17.4 需求分析与设计阶段	409
17.5 开发阶段	415
17.5.1 提供安全的函数	415
17.5.2 代码安全审计工具	417
17.6 测试阶段	418
17.7 小结	420
第18章 安全运营	422
18.1 把安全运营起来	422
18.2 漏洞修补流程	423
18.3 安全监控	424
18.4 入侵检测	425
18.5 紧急响应流程	428
18.6 小结	430
(附) 谈谈互联网企业安全的发展方向	431
. . . . .	(收起)

[白帽子讲Web安全 下载链接1](#)

标签

网络安全

安全

黑客

信息安全

计算机

互联网

web

Security

评论

准备组织组内全体同事学习此书。

还不错...少年班的人就是好

很普通阿。

有干货

:TP393.408/6843

大致翻了翻，了解下web安全中的名词术语主流应对措施。

---

@zccshome FYI

---

技术推广流...受教一部分，以后需要再来拜读

---

细读了三章。安全的本质是信任，信任圈层与信任隔离；互联网安全就是数据安全。

---

看着入门一遍挺好。就这几天捧书的时间，都被安全问题逮住撞了下腰，天意乎~~

---

还不错，不光是客观的陈述，也包含了作者的安全领域经验。但面铺的太广，有些章节就很鸡肋。而且作者对安全的理解没有深入并且贯穿的所有章节，比较可惜。显然可以写得更好

---

读这本书时回忆起了4年前摸着石头过河的经历，编码、转义、浏览器解析漏洞等一个个遇到过的线上问题历历在目，那些躲在暗处的贴吧、空间高人真有意思啊，什么都能想到，我的很多经验都是拜他们所赐。除了技术以外，个人觉得本书最后谈到的业务安全才是最头疼的，没法通过技术手段解决，防不胜防。要说挑毛病，这本书里面有很多小细节没注意，尤其是代码的排版上，另外很多地方只需要讲解原理和步骤就好了，而作者直接贴代码不讲原理，有点偷懒哦

---

鸡肋...暂时束之高阁....

---

草草读完一遍，发现以前写的代码太危险了。先略过PHP部分，看完基本的几个安全议题，毕竟自己没有在用PHP。以后肯定会再回笼看几遍。

---

网上有1,5,12章的试读，大致看了，入门，无感



-----  
服务器安全浏览一遍，加密部分没看

-----  
像作者这样年轻有为，专注安全，还能写出这样不错的书来佩服，很通俗易懂，在安全方面补了一课。

-----  
这本书还可以 适合入门

-----  
佳作

-----  
神书 值得反复研读

-----  
[白帽子讲Web安全\\_下载链接1](#)

书评

-----  
[白帽子讲Web安全\\_下载链接1](#)