

《白帽子讲Web安全（纪念版）》

图书基本信息

书名：《白帽子讲Web安全（纪念版）》

13位ISBN编号：9787121234106

出版时间：2014-6

作者：吴翰清

页数：448

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu111.com

《白帽子讲Web安全（纪念版）》

内容概要

互联网时代的数据安全与个人隐私受到前所未有的挑战，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（纪念版）》将带你走进Web安全的世界，让你了解Web安全的方方面面。黑客不再神秘，攻击技术原来如此，小网站也能找到适合自己的安全道路。大公司如何做安全，为什么要选择这样的方案呢？在《白帽子讲Web安全（纪念版）》中都能找到答案。详细的剖析，让你不仅能“知其然”，更能“知其所以然”。

《白帽子讲Web安全（纪念版）》根据安全宝副总裁吴翰清之前在顶级互联网公司若干年的实际工作经验而写成，在解决方案上具有极强的可操作性；深入分析诸多错误的方法及误区，对安全工作者有很好的参考价值；对安全开发流程与运营的介绍，同样具有深刻的行业指导意义。《纪念版》与前版内容相同，仅为纪念原作以多种语言在全球发行的特殊版本，请读者按需选用。

书籍目录

| | |
|------------------------------------|-----|
| 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: noreferrer | 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 |

《白帽子讲Web安全（纪念版）》

（附）谈谈互联网企业安全的发展方向..... 431

《白帽子讲Web安全（纪念版）》

精彩短评

- 1、从安全防护角度讲风险点。怎么说呢，纸上得来终觉浅，看是看得津津有味，书一关，熟的模块已经会了，不熟的还是不会（）。对于建立思维导图还是不错的
- 2、不错的入门书。
- 3、web安全入门，开发可以读下了解了解
- 4、十分浅显入门小白看看还可以.....换句话说就是对于想看的实际上就是并没有什么用.....还不如单刷blog.....（然而考虑到原书是3年前出版的（日新月异
- 5、入门书籍，针对一些基础CSS、sql注入会有简单的例子进行讲解。虽然内容和很多技术博客里面的内容差不了多少，但是通过书籍的汇总，至少会对web安全有一些框架的了解。
- 6、陆陆续续，反反复复。
- 7、没有想像中的好，不过还是有些有意思的内容。
- 8、入门网络安全级教程，通俗易懂
- 9、Secure by Default
- 10、推荐大家看
- 11、不是很懂里面的内容，云里雾里的，个人感觉写的深度不够，很多地方一带而过，可能是看的纪念版的缘故
- 12、想要从事Web安全的人必读的一本书。这本书对web安全方面进行了系统、全面的讲解，对于初学者更有意义。初学者应该时常翻阅的一本书。
- 13、web安全课自己买来做参考书，对于一个完全没学过安全方面知识的人来说真的很通俗易懂，配合课程的lab受益匪浅
- 14、应该算是安全的科普书。
- 15、不能说适合初学者，虽然并没有很深入，但是很系统
- 16、一个普通web码农看白帽子讲安全，期望是看到出来SQL注入和XSS之外的一些内容，偏偏这两块讲了很多很多，兴趣没那么大了。看完了，部头很大，感兴趣的内容不多，匆匆读完。
- 17、入门读本，介绍了常规的WEB安全相关知识，有较多
- 18、虽然例子可能比较老，但是还是值得一读

《白帽子讲Web安全（纪念版）》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu111.com