

白帽子讲Web安全（纪念版）



[白帽子讲Web安全（纪念版）_下载链接1](#)

著者:吴翰清

出版者:电子工业出版社

出版时间:2014-6

装帧:平装

isbn:9787121234101

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。

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)	

标签

信息安全

web安全

安全

计算机

Web安全

Web开发

黑客

security

评论

内容挺好，不过跟2012版一模一样的，“纪念版”从何而来？

1. 整体上干货不算多，通篇注重规范的讲解； 2.
能比较系统地认识安全在程序设计中的重要性； 3.
很多规则，在百度实习时有亲身体会，所以看完本书后惊喜度不高；

没有先验知识体验很差 知识没有成一个体系 太碎片化了

前端安全最佳入门

Secure by Default

看来要当好安全工程师得先学会外语逛国外论坛啊。加密算法与随机数一章没看完有空再来学习一个吧

入门网络安全级教程，通俗易懂

普普通通，查漏补缺一下

道高一尺，魔高一丈，就没有绝对安全的系统

2019-06-28：白帽子，阿里云安全负责人吴翰清的一本书，Web安全的入门书。有用是服务端安全和企业运营。可读。

挺好看的

又读了一遍，认真做笔记，有新的收获。。。

应该算是安全的科普书。

用讲常识的方式组织，因此不太结构化，每部分内容都是泛泛而谈，内容稍有些陈旧了，对毫无经验者建立概念比较适合。

陆陆续续，反反复复。

讲得很全面，干货很多，通俗易懂，诚意满满！！

很多安全概念，对于入门了解不错的

虽然例子可能比较老，但是还是值得一读

工作两年后又把这本书拿出来翻，浏览器同源策略为视角思考问题、XSS中输出环境转义、CSRF防治、生产环境的反SQL注入…比实习时有了切身和全面的了解，非常重要。
。

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

[白帽子讲Web安全（纪念版）_下载链接1_](#)

书评

内容不成体系，不熟悉的人看不懂，熟悉的人看着又没新意。
建议作者先讲基本原理，再逐步展开，这样让人理解深刻得多，否则要看这本书要准备一堆的先验知识。
但是如果已经有了先验知识，此书所讲的内容基本是安全行业的老生长谈，作者的创新在哪里？基本上是东抄西抄，还不如...

基本上覆盖了常见的安全漏洞,全书以攻-防-攻-防的脉络将web安全的要点梳理了一遍,除去框架安全漏洞,网络层安全漏洞,ddos攻击等等,常见的几种安全漏洞基本上可以以token,变量检查,特殊字符过滤,缓存设置等固定方式拦截,以前看其他部门有个开发文档,上面列出了常见安全...

此书讲述关于网络安全相关书籍,对于向我这样想了解黑客如何利用网站漏洞对站点进行攻击,有很多丰富的实例。很适合互联网的开发者,按照不同的漏洞类型进行了分类。

针对每个漏洞类型,阐述了基本概念、业界的惨痛教训、如何防范的基本技巧,不局限于某种语言,某种浏...

没有攻不破的系统,只有还没攻破的系统,有多少条路可以通罗马,大概就有多少种攻克之道。

书中一一剖析各种漏斗原理及攻防之道,既有原理分析,也有实践指导,是一本该行业从业者或是对WEB安全技术有兴趣者值得读读的书,一般看到讲安全的书,一种是讲信息安全理论体系的,基...

讲得内容很有价值,方便更整体地了解安全这个水平领域。对于程序员来说,经典代码的详解和方便操练的指导感觉还少了些,当然这样内容往往需要深入了解与一个安全点相关的知识及其工具链(如JS、SQL),这远远超出了这样一本书厚度所能承载的,应该由程序员自己去补充和深化,这...

*

一个优秀的安全方案应该具备以下特点:能够有效解决问题;用户体验好;高性能;低耦合;易于扩展与升级 *

同源策略:浏览器的同源策略,限制恶劣来自不同源的“document”或脚本,对当前“document”存期或者设置某些属性 *

互联网公司安全几个目标:第一:让工程师写出...

书中111-113页,4.2.1小结 关于Third-party Cookie(第三方Cookie)的概念解释是错误的,作者将三方Cookie和持久(Persistent)Cookie的概念弄混了。

因为看到网上没有任何人指出这个问题,这个问题又严重误导了学习者,因此我在这里纠正一下,希望有人看到。书中解释的第三方Cook...

我没有看完,只是看完了前面的web部分,服务器部分没看,因为看不懂,事实上web

部分也只能明白个大概而已。说这些只是想说明这本书不是计算机科普书。至少是对黑客攻防的一些技术和概念有些了解的人才更有用一些。其他还是看点科普文更好。虽然是说web安全，但是从攻击手段...

白帽子—防守对抗，属于“好人”

安全三要素：机密性，完整性，可用性。(这个再考虑安全的要点时，可以作为发散点) 数据从高等级的信任域流向低等级的信任域,是不需要经过安全检查的;数据从低等级的信任域流向高等级的信任域,则需要经过信任边界的安全检查。 互联网安全的...

我比较推荐日本人的写的德丸浩的web安全权威指南来入门，然后才来看这本或者那本黑皮的黑客攻防技术宝典，web实战篇，英文版。理论太多，看起来费劲，特别是初入网络安全的。最好是像德丸浩的那种书，我喜欢那种风格的，另外黑皮书也是理论多，但是黑皮书多了针对每一中类型...

也见过很多由于安全问题导致的网站损失，但往往这个东东知易行难。安全是一个相对的概念，只能用有限的资源，做尽量有效的东西。但作为一本参考书或者入门书，还是很有用的。安全这个东东，看到的权当是一种总结，或者入门。真正有价值的，还是去做。 PS.一如...

阅读时间: 2013年10月20日 -- 2013年10月23日

之前零散的看了些,这两天花时间集中的把吴翰清的这本大作看完了,真是好爽!13年安全的经验总结在这本书里,把一些web安全的本质问题一下点通,之前为了防御某种攻击而在网上找的方法也好,自己写的方法也好,其实都没有看到问题的本质,...

这本书内容很全，覆盖了web安全的前端、后端、运营等等内容，其中不仅讲解漏洞成因和原理，更提供了防御思路，这点很难得。有关安全运营的章节也很赞，这些内容只有在甲方实操过的人，才能写出干货，这也有别于市面上其他讲安全的书。缺点是，不够深入。讲的全面的书，大多不...

我没有看完，只是看完了前面的web部分，服务器部分没看，因为看不懂，事实上web部分也只能明白个大概而已。说这些只是想说明这本书不是计算机科普书。至少是对黑客攻防的一些技术和概念有些了解的人才更有用一些。其他还是看点科普文更好。虽然是说web安全，但是从攻击手段...

确实是一本不错的书。涉及到前后台的各个方面，非常好的一本初涉书籍。开篇就建立起了一个比较完整的网络安全观念，而后步步深入，从基本的一些安全概念逐渐深入到具体用例与措施。多个实例让人真正理解。感谢作者

1、web安全可以讲得东西应该还有很多。整本书看的差不多了，老感觉少了点什么东西。

2、这本书告诉了我怎么找漏洞，要怎么防范。感觉不能成功的找几个漏洞利用下，应该不算懂安全，于是拿书里面学到的方法去尝试着做点‘坏事’，漏洞确实找到了，很遗憾没有成功，我只能说实际...

第一次在文轩网买这本书，就各种不靠谱。哎，不提了。这本书挺好的，就是晚了几天读到 抱歉，你的评论太短了 抱歉，你的评论太短了 抱歉，你的评论太短了
好吧，具体就是拍下来几天之后告诉我缺货，然后就是退款各种复杂

书是好书,可为什么没有目录? 为了安全么? 安全专家的书籍果然不一样 好吧,我自己印一个目录贴进去好了 书是好书,可为什么没有目录? 为了安全么? 安全专家的书籍果然不一样 好吧,我自己印一个目录贴进去好了 书是好书,可为什么没有目录? 为了安全么? 安全专家...

[白帽子讲Web安全（纪念版）_下载链接1](#)