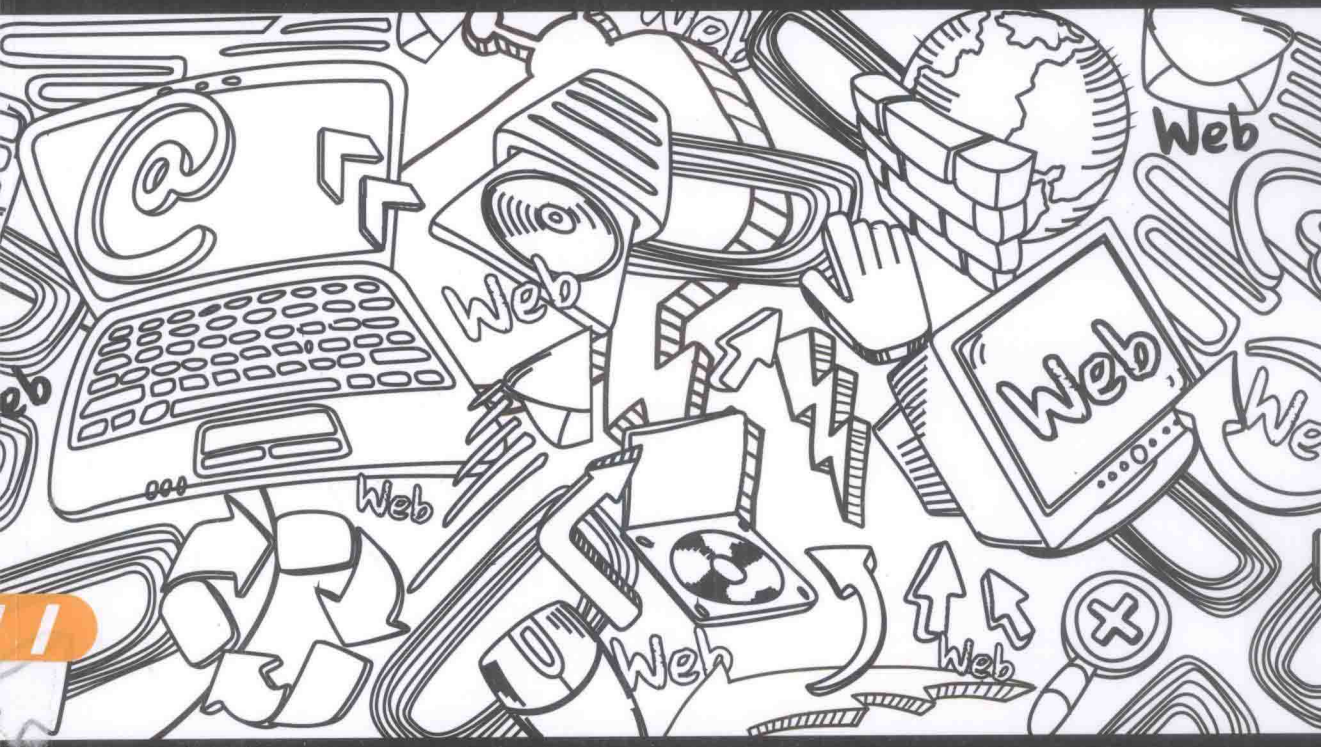
Broadview
www.broadview.com.cn

剖析Web安全核心技术，提出完善的检测与防御方案，让入侵者无处遁形

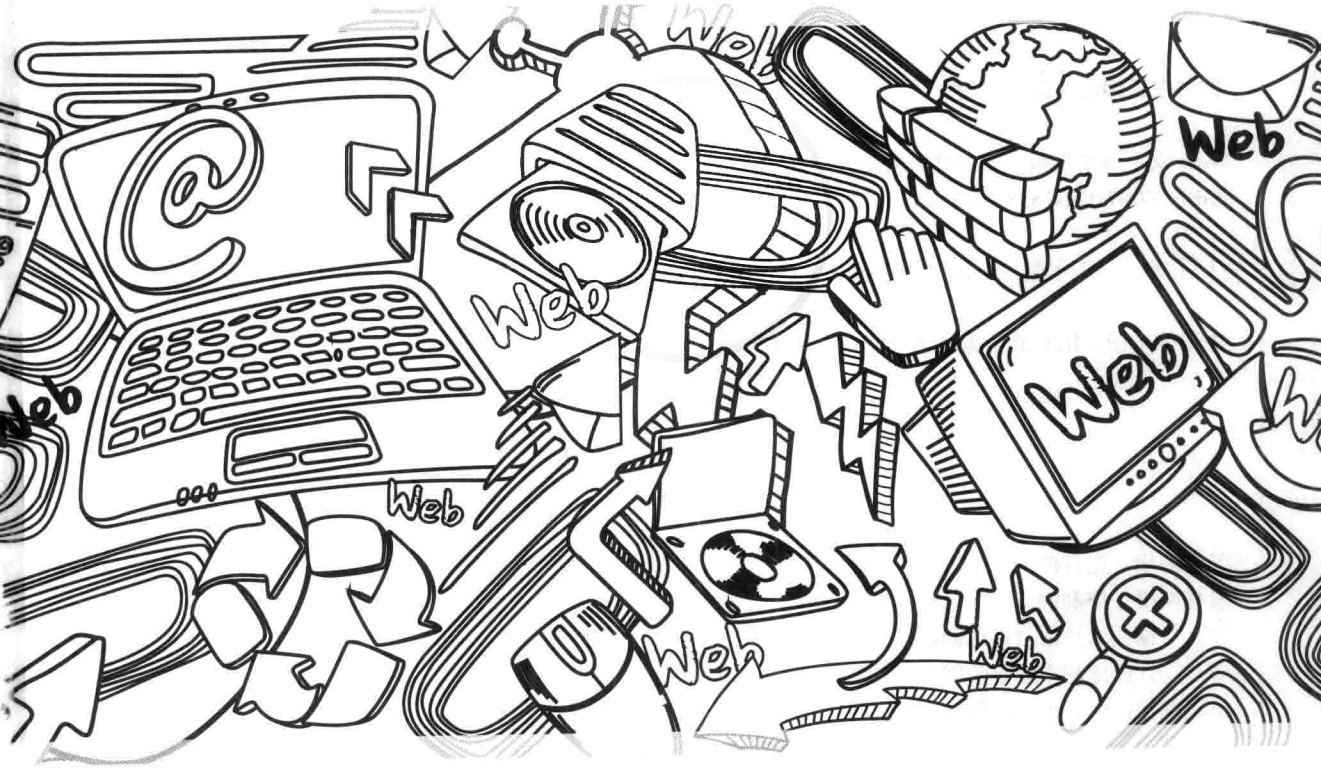
Web安全深度剖析



张炳帅 编著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

Web安全深度剖析



张炳帅　编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书总结了当前流行的高危漏洞的形成原因、攻击手段及解决方案，并通过大量的示例代码复现漏洞原型，制作模拟环境，更好地帮助读者深入了解 Web 应用程序中存在的漏洞，防患于未然。

本书从攻到防，从原理到实战，由浅入深、循序渐进地介绍了 Web 安全体系。全书分 4 篇共 16 章，除介绍 Web 安全的基础知识外，还介绍了 Web 应用程序中最常见的安全漏洞、开源程序的攻击流程与防御，并着重分析了“拖库”事件时黑客所使用的攻击手段。此外，还介绍了渗透测试工程师其他的一些检测方式。

本书最适合渗透测试人员、Web 开发人员、安全咨询顾问、测试人员、架构师、项目经理、设计等人员阅读，也可以作为信息安全等相关专业的教材。

图书在版编目（CIP）数据

Web 安全深度剖析 / 张炳帅编著. —北京：电子工业出版社，2015.4
ISBN 978-7-121-25581-6

Ⅰ.①W… Ⅱ.①张… Ⅲ.①互联网络－安全技术 Ⅳ.①TP393.408

中国版本图书馆 CIP 数据核字（2015）第 036493 号

策划编辑：张月萍
责任编辑：李利健
印　　刷：涿州市京南印刷厂
装　　订：涿州市京南印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×1092　1/16　印张：22.5　字数：590 千字
版　　次：2015 年 4 月第 1 版
印　　次：2015 年 4 月第 1 次印刷
印　　数：3500 册　　定价：59.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

推荐序

纵观国内网络安全方面的书籍，大多数都是只介绍结果，从未更多地考虑过程。而本书恰恰是从实用角度出发，本着务实的精神，先讲原理，再讲过程，最后讲结果，是每个从事信息安全的从业人员不可多得的一本实用大全。尤其是一些在企业从事信息安全的工作人员，可以很好地依据书中的实际案例进行学习，同时，在校学生也可以依据本书的案例进行深入学习，有效地贴近企业，更好地有的放矢。

——陈亮　OWASP 中国北京主负责人

我有幸见证了《Web 安全深度剖析》诞生的全过程，作者认真严谨的写作风格，深入求证的研究态度，深厚的程序员功底，丰富的网络和现场教育培训经验，使本书成为适合 Web 渗透测试的必选作品。本书内容丰富，知识点全面，适合网络安全爱好者和从业者学习研究。

——一剑西来　红黑联盟站长，暗影团队管理员

我收到《Web 安全深度剖析》样章后，一口气通读下来，感觉酣畅淋漓。作者用深入浅出的手法，贴近实战，基本涵盖了 Web 安全技术中实际遇到的方方面面。本书适合 Web 安全从业人员研读，也推荐有志在 Web 安全方向发展的人学习。

——lake2　腾讯安全平台部副总监

与其说这是一本 Web 安全的书籍，不如说是一本渗透实战教程，该书总结了不少常见的 Web 渗透思路和奇技淫巧，非常适合初学者和有一些基础的人阅读。安全圈有一句老话：未知攻，焉知防。这本书可以帮助大家找到学习安全知识的兴趣，也可以找到学习安全知识的方法。

——林伟（网名：陆羽）

360 网络攻防实验室负责人，国内知名安全社区 T00ls.net 创始人之一

本书根据作者多年工作经验积累写成，作者从一个渗透测试者的角度，深入浅出地剖析了一个网站或一家企业会遇到的安全问题。最终本书解答了一个很多人感兴趣的问题：服务器到底是怎么被黑掉的？相信这对所有开展互联网业务的公司，以及所有想从事安全行业的初学者来说，都是一本很好的学习指南。

——吴翰清　阿里巴巴集团研究员，《白帽子讲 Web 安全》作者

终于等到张炳帅这本书了，他拥有非常丰富的实战经验，这本书里的“干货”绝对值得细细品味，我期待已久！

——余弦　知道创宇技术副总裁

《Web 安全深度剖析》书如其名，是一本极具实用性、贴近实战的 Web 安全指导书籍，覆盖了 Web 渗透测试中实际遇到的各类安全漏洞、利用技巧和攻击场景，能够帮助安全从业者和爱好者快速了解并建立 Web 渗透测试所需的知识与技能，值得深入研读。

——诸葛建伟　清华大学副研究员，蓝莲花战队领队

前　言

本书总结了当前流行的高危漏洞的形成原因、攻击手段及解决方案，并通过大量的示例代码复现漏洞原型，制作模拟环境，更好地帮助读者深入了解 Web 应用程序中存在的漏洞，防患于未然。

本书抛开一些研究性、纯理论性的内容，也就是外表看似很高端，但实用性不大的课题，所总结的漏洞知识可以说是刀刀见血、剑剑穿心。漏洞直接危害到企业的安全。

本书也是笔者多年来的工作总结，几乎每个场景都是最常见的，如果你从事与 Web 渗透测试相关的工作，就会遇到本书中的场景。

本书结构

本书从攻到防，从原理到实战，由浅入深、循序渐进地介绍了 Web 安全体系。全书分 4 篇共 16 章，这是一个庞大的体系，几乎可以囊括目前常见的一切 Web 安全类技术。

本书目录结构就非常像渗透测试人员的一次检测流程，从信息探测到漏洞扫描、漏洞利用、提权等。

基础篇

第 1 章到第 4 章为基础篇，是整个 Web 安全中最基础的技术。

第 1 章描述了服务器是如何被黑客入侵的，并从中引出 Web 安全的概念，同时也告诉读者如何更快、更好地学习 Web 安全。

第 2 章详细讲述了 Web 安全的一个核心知识点：HTTP 协议。如果是零基础的读者，建议一定要多看 HTTP 协议，因为后续章节中的许多内容都会涉及 HTTP 协议。

第 3 章介绍了信息探测的知识点。渗透测试人员工作时，一般都是从信息探测入手的，也就是常说的踩点。信息探测是渗透测试的基本功，是必须学习的内容。本章介绍了 Google Hack、Nmap、DirBuster、指纹识别等技术。

第 4 章讲解了渗透测试人员常用的安全测试工具，包括：BurpSuite、AWVS、APPSCAN 等工具。

原理篇

第 5 章到第 10 章为原理篇，阅读本篇内容需要读者具备一定的代码功底。在这些章节中讲述了 Web 应用程序中最常见的安全漏洞。笔者将这些常见的高危漏洞提取出来，每个漏洞作为单独的一个章节来讲解，从原理到利用。

第 5 章是 SQL 注入章节，讨论了 MySQL、SQL Server、Oracle 数据库的注入方式、注入技巧和不同数据库的注入差异。

攻击者对数据库注入的目的有：数据窃取、文件读写、命令执行。掌握其核心思想后，对 SQL 注入的学习就比较容易了。

在讲解 SQL 注入原理后，介绍了 SQLMap、Havij 等注入工具，同时也介绍了绕过部分 WAF 的思路。

第 6 章介绍了 XSS 攻击，其中讲解了 XSS 的形成原理、三种 XSS 类型、会话劫持、蠕虫等前端技术，最后提出了 XSS 有效的解决方案。

第 7 章讲解了上传漏洞和 Web 容器的漏洞。有时候程序是没有问题的，但如果与 Web 容器漏洞相结合，可能就会造成上传漏洞。

第 8 章描述了命令执行漏洞的形成原因和利用方式，同时也介绍了 Struts2 命令执行漏洞及命令执行漏洞的修复方案。

第 9 章讲解了 PHP 包含漏洞的原理和利用方式，同时也介绍了包含漏洞的修复方案。

第 10 章讨论的知识点比较广泛，比如 CSRF、逻辑漏洞、远程部署漏洞、代码注入等高危漏洞。

实战篇

第 11 章讲述了开源程序的攻击流程与防御，并着重分析了“拖库”事件时黑客所使用的攻击手段。

综合篇

如果仅仅掌握 Web 安全漏洞，而对其他漏洞、攻击手法一窍不通，是无法全面找出漏洞的。本书在综合篇里介绍了渗透测试工程师的一些其他检测方式。

第 12 章详细讲述了暴力破解的测试方式，分别使用 Hydra、Burp Suite、Medusa 等工具对 MSSQL、MySQL、Web 应用程序进行破解，最后讲述了验证码的安全性及防止暴力破解的解决方案。

第 13 章讲述了旁注攻击。当目标 Web 应用程序无法寻找到漏洞时，攻击者常常会使用旁注攻击来入侵目标。本章剖析了旁注攻击的几个关键点，包括 IP 逆向查询、SQL 跨库查询、绕

过 CDN 等技术。

第 14 章讲述了提权。服务器提权可以更好地解释服务器的脆弱性，本章对 Linux、Windows 提权均做了分析。比如 Windows 下的三种提权方式：本地溢出提权、第三方组件提权和系统关键点利用。另外，也剖析了一部分提权时的采用手段，比如 DLL 劫持、端口转发、服务器添加后门等技术。

第 15 章讲述了 ARP 攻击与防御。安全是一个整体，并不是 Web 应用程序找不到漏洞时，黑客就没办法了，黑客使用 ARP 欺骗技术可以轻松劫持到你的密码。本章从 ARP 协议开始讲解，接着深入讲解 ARP 欺骗的原理，其中介绍了 Cain、Ettercap、NetFuke 等嗅探工具。

第 16 章讲述了社会工程学。社会工程学可以说是 APT 攻击中的关键一环，也被称为没有“技术”却比“技术”更强大的渗透方式。

需要的工具

本书的核心是从原理到实战案例的剖析，很多时候，工具只是起辅助作用。读者要注意一点：在实际的渗透中，更多地靠经验、思路，工具反而是其次，不要被众多的“神器”所迷惑。工具仅仅是让我们更方便、高效一些，工具是“死”的，目前的软件开发水平还完全达不到智能化，工具只能按照程序员的思维流程来执行。所以，我们完全依赖的还是自己的大脑。

本书所使用的工具可以在 http://www.secbug.org/tools/index.html 中下载。

本书是写给谁的

本书最适合渗透测试人员、Web 开发人员、安全咨询顾问、测试人员、架构师、项目经理、设计等人员阅读，也可以作为 Web 安全、渗透测试的教材。这是一本实用的 Web 安全教材。

- 渗透测试人员：渗透测试人员要求具备的技术在大学并没有课程设置，也没有正规、专业的技术培训。可以说，做渗透测试的人员都要靠自学，付出比其他人更多的努力才能胜任这个工作。笔者希望读者从本书中学到知识，进一步提高自己的渗透测试水平。
- Web 开发人员：程序员不一定是黑客，但是有一定水平的黑客、白帽子一定是程序员。因此，一个合格的程序员学习安全知识是非常快的。本书介绍了大量的示例代码，并分析了其中的漏洞，从开发人员的角度讲述如何避免和修复漏洞，希望开发人员能够通过本书的学习提高自己防御安全的水平，站在新的高度去看待程序。
- 信息安全相关专业的学生：本书也适合信息安全等相关专业的学生阅读，书中所有的知识点几乎都是从零开始的，你们可以循序渐进地学习。同时，笔者也希望能给大学老师带来一些灵感，然后培育出更多的网络安全人才。

在学习时，笔者常把原理性的知识比喻为内功，而具体的实操、技术点比喻为招式，只有招式而没有内功是根本无法变成高手的，有了内功和招式才可能成为高手。

安全是把双刃剑。剑在手中，至于是用其来做好事还是做坏事，只在于一念之差。笔者强烈要求各位读者仅在法律的许可范围内使用本书所提供的信息。

致谢

感谢 EvilShad0w 团队的每一位成员，你们在一起交流技术、讨论心得时从来都是无私地分享，你们都有一颗对技术狂热的心。在我眼里，你们都是“技术帝”。

感谢破晓团队的每一位成员，感谢你们相信我，愿意跟我一起闯，你们的存在是支撑我继续下去的力量。

感谢联合实验室的成员，是你们在百忙之中细细品味这本书，并指出不足之处。

感谢袁海君、杜萌萌、LiuKer、7z1、天蓝蓝、小 K、小歪、岩少、晴天小铸、GBM 的支持。有你们的支持，我才能完成这本书的写作，也感谢你们对这本书做出的贡献，我将谨记于心。这里要特别感谢小杜，你为我审阅稿子，找出书中的许多错误。

感谢红黑联盟站长一剑西来、天云祥科技有限公司 CEO 杨奎，你们给了我许多机会，也教会了我如何去思考。

感谢我的领导沈局、邬江、邓小刚，你们对待我就像对待自己的学生一样，给了我许多教导。

最后，感谢我的父母，感谢你们将我抚育成人，为我付出一切。这份爱时刻提醒着我，要努力、要上进！

路虽艰，行则必达。事虽难，做则必成。

破晓-SecBug.Org

目　录

第 1 篇　基础篇

第 1 章　Web 安全简介 …… 2

1.1　服务器是如何被入侵的 …… 2

1.2　如何更好地学习 Web 安全 …… 4

第 2 章　深入 HTTP 请求流程 …… 6

2.1　HTTP 协议解析 …… 6

2.1.1　发起 HTTP 请求 …… 6

2.1.2　HTTP 协议详解 …… 7

2.1.3　模拟 HTTP 请求 …… 13

2.1.4　HTTP 协议与 HTTPS 协议的区别 …… 14

2.2　截取 HTTP 请求 …… 15

2.2.1　Burp Suite Proxy 初体验 …… 15

2.2.2　Fiddler …… 19

2.2.3　WinSock Expert …… 24

2.3　HTTP 应用：黑帽 SEO 之搜索引擎劫持 …… 24

2.4　小结 …… 25

第 3 章　信息探测 …… 26

3.1　Google Hack …… 26

3.1.1　搜集子域名 …… 26

3.1.2　搜集 Web 信息 …… 27

3.2　Nmap 初体验 …… 29

3.2.1　安装 Nmap …… 29

3.2.2　探测主机信息 …… 30

3.2.3　Nmap 脚本引擎 …… 32

3.3 DirBuster ····· 33
3.4 指纹识别 ····· 35
3.5 小结 ····· 38
第 4 章 漏洞扫描 ····· 39
4.1 Burp Suite ····· 39
4.1.1 Target ····· 39
4.1.2 Spider ····· 40
4.1.3 Scanner ····· 42
4.1.4 Intruder ····· 43
4.1.5 辅助模块 ····· 46
4.2 AWVS ····· 49
4.2.1 WVS 向导扫描 ····· 50
4.2.2 Web 扫描服务 ····· 52
4.2.3 WVS 小工具 ····· 53
4.3 AppScan ····· 54
4.3.1 使用 AppScan 扫描 ····· 55
4.3.2 处理结果 ····· 58
4.3.3 AppScan 辅助工具 ····· 58
4.4 小结 ····· 61

第 2 篇 原理篇

第 5 章 SQL 注入漏洞 ····· 64
5.1 SQL 注入原理 ····· 64
5.2 注入漏洞分类 ····· 66
5.2.1 数字型注入 ····· 66
5.2.2 字符型注入 ····· 67
5.2.3 SQL 注入分类 ····· 68
5.3 常见数据库注入 ····· 69
5.3.1 SQL Server ····· 69
5.3.2 MySQL ····· 75
5.3.3 Oracle ····· 84
5.4 注入工具 ····· 89
5.4.1 SQLMap ····· 89
5.4.2 Pangolin ····· 95
5.4.3 Havij ····· 98
5.5 防止 SQL 注入 ····· 99
5.5.1 严格的数据类型 ····· 100

5.5.2 特殊字符转义 101
5.5.3 使用预编译语句 102
5.5.4 框架技术 103
5.5.5 存储过程 104
5.6 小结 105
第 6 章 上传漏洞 106
6.1 解析漏洞 106
6.1.1 IIS 解析漏洞 106
6.1.2 Apache 解析漏洞 109
6.1.3 PHP CGI 解析漏洞 110
6.2 绕过上传漏洞 110
6.2.1 客户端检测 112
6.2.2 服务器端检测 115
6.3 文本编辑器上传漏洞 123
6.4 修复上传漏洞 127
6.5 小结 128
第 7 章 XSS 跨站脚本漏洞 129
7.1 XSS 原理解析 129
7.2 XSS 类型 130
7.2.1 反射型 XSS 130
7.2.2 存储型 XSS 131
7.2.3 DOM XSS 132
7.3 检测 XSS 133
7.3.1 手工检测 XSS 134
7.3.2 全自动检测 XSS 134
7.4 XSS 高级利用 134
7.4.1 XSS 会话劫持 135
7.4.2 XSS Framework 141
7.4.3 XSS GetShell 144
7.4.4 XSS 蠕虫 149
7.5 修复 XSS 跨站漏洞 151
7.5.1 输入与输出 151
7.5.2 HttpOnly 158
7.6 小结 160
第 8 章 命令执行漏洞 161
8.1 OS 命令执行漏洞示例 161
8.2 命令执行模型 162

8.2.1 PHP 命令执行 163
8.2.2 Java 命令执行 165
8.3 框架执行漏洞 166
8.3.1 Struts2 代码执行漏洞 166
8.3.2 ThinkPHP 命令执行漏洞 169
8.4 防范命令执行漏洞 169
第 9 章 文件包含漏洞 171
9.1 包含漏洞原理解析 171
9.1.1 PHP 包含 171
9.1.2 JSP 包含 180
9.2 安全编写包含 184
9.3 小结 184
第 10 章 其他漏洞 185
10.1 CSRF 185
10.1.1 CSRF 攻击原理 185
10.1.2 CSRF 攻击场景（GET） 186
10.1.3 CSRF 攻击场景（POST） 188
10.1.4 浏览器 Cookie 机制 190
10.1.5 检测 CSRF 漏洞 193
10.1.6 预防跨站请求伪造 197
10.2 逻辑错误漏洞 199
10.2.1 挖掘逻辑漏洞 199
10.2.2 绕过授权验证 200
10.2.3 密码找回逻辑漏洞 204
10.2.4 支付逻辑漏洞 205
10.2.5 指定账户恶意攻击 209
10.3 代码注入 210
10.3.1 XML 注入 211
10.3.2 XPath 注入 212
10.3.3 JSON 注入 215
10.3.4 HTTP Parameter Pollution 216
10.4 URL 跳转与钓鱼 218
10.4.1 URL 跳转 218
10.4.2 钓鱼 220
10.5 WebServer 远程部署 224
10.5.1 Tomcat 224
10.5.2 JBoss 226

10.5.3　WebLogic ····· 229
10.6　小结 ····· 233

第 3 篇　实战篇

第 11 章　实战入侵与防范 ····· 236
11.1　开源程序安全剖析 ····· 236
11.1.1　0day 攻击 ····· 236
11.1.2　网站后台安全 ····· 238
11.1.3　MD5 还安全吗 ····· 243
11.2　拖库 ····· 248
11.2.1　支持外连接 ····· 248
11.2.2　不支持外连接 ····· 253
11.3　小结 ····· 262

第 4 篇　综合篇

第 12 章　暴力破解测试 ····· 264
12.1　C/S 架构破解 ····· 265
12.2　B/S 架构破解 ····· 272
12.3　暴力破解案例 ····· 275
12.4　防止暴力破解 ····· 277
12.5　小结 ····· 278
第 13 章　旁注攻击 ····· 279
13.1　服务器端 Web 架构 ····· 279
13.2　IP 逆向查询 ····· 280
13.3　SQL 跨库查询 ····· 282
13.4　目录越权 ····· 283
13.5　构造注入点 ····· 284
13.6　CDN ····· 286
13.7　小结 ····· 288
第 14 章　提权 ····· 290
14.1　溢出提权 ····· 290
14.2　第三方组件提权 ····· 294
14.2.1　信息搜集 ····· 294
14.2.2　数据库提权 ····· 296
14.2.3　FTP 提权 ····· 302
14.2.4　PcAnywhere 提权 ····· 312
14.3　虚拟主机提权 ····· 314

14.4 提权辅助……315
14.4.1 3389 端口……315
14.4.2 端口转发……318
14.4.3 启动项提权……320
14.4.4 DLL 劫持……321
14.4.5 添加后门……322
14.5 服务器防提权措施……324
14.6 小结……325
第 15 章 ARP 欺骗攻击……326
15.1 ARP 协议简介……326
15.1.1 ARP 缓存表……326
15.1.2 局域网主机通信……327
15.1.3 ARP 欺骗原理……328
15.2 ARP 攻击……329
15.2.1 Cain……329
15.2.2 Ettercap……332
15.2.3 NetFuke……336
15.3 防御 ARP 攻击……339
15.4 小结……340
第 16 章 社会工程学……341
16.1 信息搜集……341
16.2 沟通……343
16.3 伪造……344
16.4 小结……345
严正声明……346

第 1 篇

基础篇

- 第 1 章　Web 安全简介
- 第 2 章　深入 HTTP 请求流程
- 第 3 章　信息探测
- 第 4 章　漏洞扫描

第 1 章

Web 安全简介

1.1 服务器是如何被入侵的

在介绍 Web 安全的内容之前，我们先了解一下一台在互联网中的服务器是如何被攻击者入侵的。

攻击者想要对计算机进行渗透，有一个条件是必需的：就是攻击者的计算机与服务器必须能够正常通信。服务器提供各种服务供客户端使用，那么此时服务器是如何与客户端通信的？依靠的就是端口。攻击者入侵也是靠端口，或者说是计算机提供的服务。当然不排除一些“物理黑客”，直接进入服务器所在的机房对服务器动手。

过去的黑客攻击方式大多数都是直接针对目标进行攻击，比如端口扫描、一些服务的密码爆破（如：FTP、数据库）、缓冲区溢出攻击等方式直接获取目标权限，在 2000 年至 2008 年，使用溢出软件扫描主机，在 100 台计算机中可能会有 20 台计算机中招，可见服务器有多么脆弱。如今，这种直接对服务器进行溢出攻击的方式越来越少，因为系统的溢出漏洞太难挖掘了，新的战场已转移到 Web 之上。

早期的互联网是非常单调的，一般只有静态的文档，随着技术的发展，互联网慢慢变得多姿多态，每个人都可以在互联网中遨游，向网友“诉说”。小学时教科书上所说的“地球村”也真正实现了。

如今的 Web 应该称之为 Web 应用程序，与早期的 Web 有天壤之别，如今的 Web 功能非常强大，网上购物、办公、游戏、社交等活动都不在话下，而使用者（客户端）需要做的仅仅是拥有一个浏览器，就可做到这么多任务。

是什么让 Web 如此强大？它离不开四个要点：数据库、编程语言、Web 容器和优秀的 Web 应用程序的设计者，这四个缺一不可。

优秀的设计人员设计个性化的程序，编程语言将这些设计变为真实的存在，且悄悄地与数据库连接，让数据库存储好这些数据，而 Web 容器负责的则是作为终端解析用户请求和脚本语言等。当用户通过统一资源定位符（URL）访问 Web 时，最终看到的是 Web 容器处理后的内