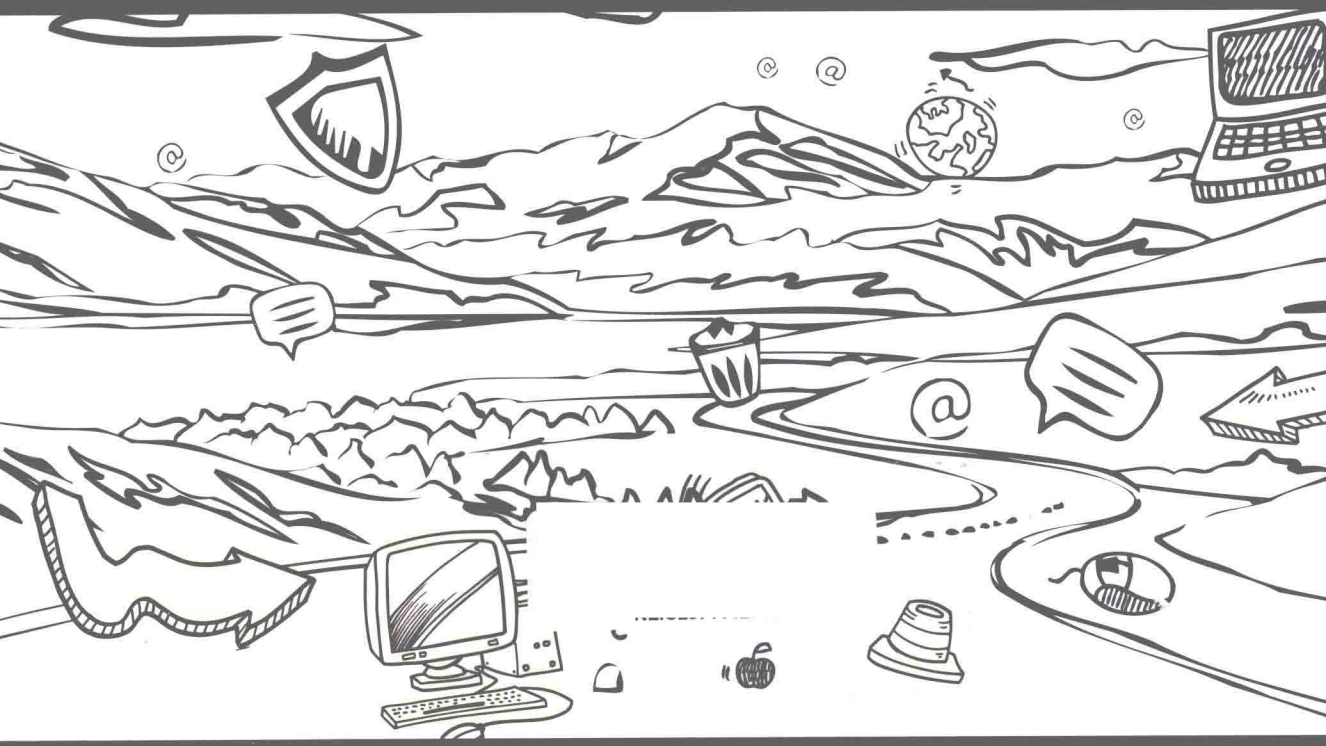
Broadview
www.broadview.com.cn

安全技术大系

案例全解Web渗透技术，实战，实战，再实战！

安全之路

Web渗透技术及实战案例解析 第2版



陈小兵 编著

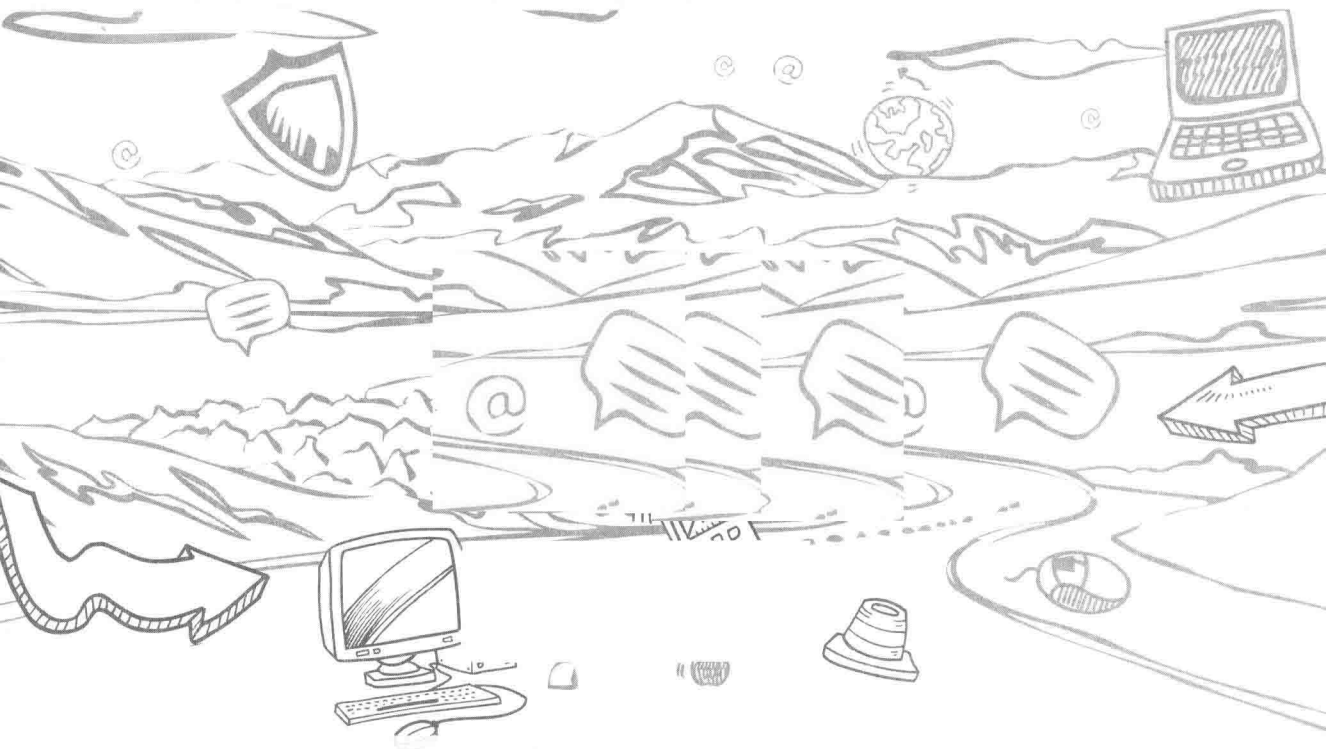
中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

安全之路

Web渗透技术及实战案例解析 第2版

陈小兵 编著



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

内 容 简 介

本书是《Web 渗透技术及实战案例解析》一书的第 2 版。本书从 Web 渗透的专业角度，结合网络攻防中的实际案例，图文并茂地再现了 Web 渗透的精彩过程。本书还精选经典案例，搭建测试环境，供读者进行测试。本书较第 1 版更加系统、科学地介绍了各种渗透技术，由浅入深地介绍和分析了目前网络上流行的 Web 渗透攻击方法和手段，并结合作者多年的网络安全实践经验给出了相应的安全防范措施，对一些经典案例还给出了经验总结和技巧归纳。本书最大的特色是实用性高、实战性强、思维灵活，内容主要包括 Web 渗透必备技术、常见的加密与解密攻击、Web 漏洞扫描、常见的文件上传漏洞及利用、SQL 注入漏洞及利用、高级渗透技术、Windows 和 Linux 提权、Windows 和 Linux 的安全防范等。

本书既可以作为政府、企业网络安全从业者的参考资料，也可以作为大专院校学生学习渗透测试的教材。

图书在版编目（CIP）数据

安全之路：Web 渗透技术及实战案例解析 / 陈小兵编著. —2 版. —北京：电子工业出版社，2015.9
（安全技术大系）

ISBN 978-7-121-26774-1

Ⅰ. ①安… Ⅱ. ①陈… Ⅲ. ①计算机网络—安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2015）第 169571 号

责任编辑：潘 昕
印 刷：北京丰源印刷厂
装 订：三河市皇庄路通装订厂
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：36.5 字数：880 千字
版 次：2012 年 4 月第 1 版
2015 年 9 月第 2 版
印 次：2015 年 9 月第 1 次印刷
定 价：99.00 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。

序 1

我和小兵相识多年。他起初作为《黑客防线》的读者，而后作为《黑客防线》的作者，在十几年的时间里，虽经历过工作变动，其间还有几年去读研究生，但始终没有脱离和《黑客防线》技术团队的关系。多年来，他的兴趣和主要钻研的技术领域一直都在网络安全方面，特别是 Web 安全领域。对于一个既无学科传承，又无技术体系的全新领域，一头扎进去就是十几年，这在近乎杂乱和浮躁的网络技术行业实属少见。这是他的兴趣，更重要的是，他似乎感觉到，在网络时代，网络安全始终是一个无法回避的重大问题，是一个需要正面积极应对的问题，此中他感受到除了兴趣以外的一种责任，这可能是我们能成为知音且一直保持联系的原因所在。

起初，我们这些专注于系统底层和协议底层技术的人，对于 Web 层面的安全技术并不是那么看重，但是，随着 Web2.0 技术的广泛应用，网络大架构普遍与 Web 服务器直接或者间接互连互通，其现实变为 Web 服务器不仅可以到达外网数据库，也可以到达内网，甚至可以到达骨干网节点——当今世界，完全封闭运行的局域网已经非常少见，这使我们逐渐认识到，Web 攻击和渗透非常有效，因此，Web 安全防范技术显得非常重要。这也正是小兵一直坚持探索的价值所在。

其实，网络安全面临的形势远比我们所知严峻得多。尽管斯诺登已经披露了很多，几乎等于一场网络安全普及教育；尽管我们已经亲历震网、火焰这样攻击代码的分析，几乎等于一堂技术提高课——但是，我们的危机感仍远远不够。大到国家重要数据，中到重要商业数据，小到个人隐私数据，只要这些数据存在于数字设备中，只要这些数字设备存在于网络中，就等于开通了无数个获取核心数据的通道。能否做到有效防范，其根本毋庸置疑，就是技术的比拼，其原理就是我为《黑客防线》确定的核心理念：在攻与防的对立统一中寻求技术突破。小兵及他所带领的团队正是在这个理念下一直坚持探索，取得了不少技术成果，这是我的欣慰，也是中国网络安全的幸事。当初，小兵作为我的“小伙伴”走上了这条路，后来，他又带领不同阶段的小团队，一直在 Web 安全技术上不停探索，更是网络安全技术领域珍贵的后备力量。

“路漫漫其修远兮”，愿小兵及他的后续团队能够一路走下去。还是当年那句话：我们的技术刚刚起步。

孙　彬

《黑客防线》总编辑

序 2

这本书是我非常推荐的一本 Web 渗透书籍。这些年来，小兵一直潜心沉淀，在我眼里，他是一线的实战派！这本书的第 1 版面世时，我就第一时间拿到手，当时很是惊讶——作为一线人员的他将多年的积累写成了书。现在的第 2 版更是让人刮目相看。所以，当他说希望我能为这本书写序的时候，我非常爽快地答应下来，希望能向大家传达一些特别的见解。

我和小兵是老朋友了，每次坐下来聊天时，都会碰撞出渗透的火花，这一点让我很是受用。在黑客渗透领域，Web 渗透是一个极其重要的分支。从这本书中可以看出，小兵最擅长的是 Web 服务端渗透，包括从拿下 Web 服务到进入服务器、进入内网的许多渗透思路，这个过程中还融入了社会工程学的经典应用，这些经验非常值得借鉴。但是，这本书没有提到 Web 客户端（或称“Web 前端”）的渗透，最近全球范围内大量报道的“水坑”攻击，其实就是一种 Web 客户端的攻击思路，其中一个典型应用就是 XSS 攻击。在我看来，XSS、CSRF 等 Web 客户端技术在真实的渗透中也是非常有效的，例如大家熟知的“XSS 盲打技术”。Web 客户端的渗透其实是一种被动渗透的思路，往往需要精心准备攻击页面（经常携带恶意 JavaScript 代码），然后通过精准的社工手法或“盲打”技术将这个攻击页面发给目标用户，等待目标用户主动或被动访问这个攻击页面，只要目标用户的浏览器请求访问这个攻击页面，就可以触发这个页面携带的恶意 JavaScript 代码。这段代码不可小觑，很可能让我们坠入“大水坑”，导致 Web 账号甚至机器（PC 或手机）被控制等许多意想不到的结果。

小兵分享的 Web 渗透经验是一种主动渗透思路，这和 Web 客户端的被动渗透思路很不一样。虽然在我看来这两种思路都很重要，但在真实的渗透过程中，主动渗透思路却是主角。希望大家能用心吸收本书的经验，并在实战中发散自己的思路——如果未来的某一天有机会碰面聊天，我们可以一起碰撞出更多新的火花。

最后，由衷钦佩小兵的敬业精神与分享精神，一起加油！

余　弦

《Web 前端黑客技术揭秘》作者

序3

其实我和小兵认识的时间不算太长，记得是在他写这本书的第 1 版时，通过好朋友兼前同事“鸟哥”认识的。我对小兵的第一印象是——实在，肯深入钻研各种安全渗透技术，交流的都是“干货”，所以很愿意和他交流分享，互相学习进步。现在，这本书的第 2 版又让我受益匪浅。

当前，信息安全很火，Web 安全更火，各行业、各公司都很重视 Web 安全，对这方面的人才需求很大，所以，这方面的书也很多，有讲原理的，有说框架的，有介绍工具的，也有讲实际操作的，但很少能像这本书一样，由浅入深，全面而深入地介绍和分析当前的渗透技术和手段，着重介绍实际操作、经验和技巧——还有一些是独门绝技。

在小兵写这本书的过程中，我们有一些交流，感觉他对这本书非常认真、仔细，书里的每个工具、案例、技巧都必须在测试环境里测试通过，不确定的坚决不用。我想，这也许是这本书成为一本高质量 Web 安全书籍的重要原因吧！

期待小兵及其团队写出更多更好的安全书籍，和大家一起分享你们的宝贵经验。

张　健

完美世界信息安全总监

序 4

计算机安全的涉及范围非常广，Web 安全是其中之一，渗透测试技术也是 Web 安全领域非常热门的技术之一。相比传统的软件安全，Web 安全入门的门槛要低很多，而且相对更容易让我们体验渗透测试带来的乐趣。对渗透测试的技术能力来说，最大的价值不是使用的工具，而是实战经验。在渗透测试中，思路和经验往往比工具、0day 更重要，这本书就分享了大量的实战经验，大家可以好好吸收。

我在甲方做安全业务将近 5 年，期间也写过 4 本安全技术书籍，对安全行业的认识达到了一定的程度。对企业来说，一个合适的安全技术人才非常难以招募。我们通常会开出很高的薪酬待遇，但仍然很难招到我们需要的人才。产品和业务的安全对企业来说至关重要，一个很小的漏洞就可造成无法预估的重大影响。以微博业务为例，任何一个有影响力的“大 V”账户被盗所导致的不良言论，就可能导致公司股价的波动，而“大 V”账户被盗的可能性众多，我们需要防护的点也非常多。安全体系遵循木桶原理，即使其他方面做得再好，只要某个细小的方面出现问题，就会导致整个安全体系的崩溃。

小兵是我很要好的朋友，他一直在渗透测试领域保持着较高的技术水平。很高兴看到小兵这本书出版第 2 版。相比第 1 版，第 2 版增加了大量实战案例，图文并茂，读者可以根据这些实例不断加深自己的理解，丰富自己的渗透测试经验。

总之，这是一本充满实战经验的 Web 安全相关书籍，对于刚刚接触渗透测试技术的朋友来说，通篇没有多余的理论铺垫，就像书名强调的那样——注重实战，相信读完一定收获颇多。

如果你有兴趣与我们一起建立一套完善的社交网络防护安全体系，不妨把简历发给我（shiyao@staff.weibo.com），我们相约北京。

罗诗尧

新浪微博安全团队负责人

序5

随着互联网的飞速发展和 Web 技术的日新月异，特别是 Web2.0 的普及和发展，Web 应用的功能越来越强大，而与之相关的网络安全问题也让人目不暇接：CSDN 用户信息泄露、天涯论坛数据泄露、小米数据泄露、Gmail 数据泄露……呈愈演愈烈之势。Web 安全已经逐渐成为当今网络安全最热门的领域之一，在近年举国上下重点关注安全之际，本书的面世为我们带来了新的“技术食粮”——向陈小兵同志致敬！

我和挚友小兵从认识到现在已有 8 年之久，今日他的杰作第 2 版即将出版，我心中充满喜悦之情，这既是众多网友的期待，也使我们信息安全网络学院学员们的呼声又一次得到满足。小兵为人厚道，做事认真，在国内信息安全圈子中享有盛名，但他为我的助理和网络学员们解答问题时又是那么和蔼可亲，堪称“技术大牛型笑脸哥”，此书一出，学员们估计又要托我来买签名书了。小兵历尽心血更新的第 2 版融入了大量渗透思路和实战经验，并将书中重要的实验放到我主持研发的“红黑演义云端攻防平台”上供大家实践，更体现了他对读者的厚爱！

小兵在 Web 安全领域研究和工作多年，积累了丰富的理论和实战经验，这本书正是这些宝贵经验的结晶。系统性和科学性是本书的第一大特点，本书内容既涵盖了 Web 渗透技术和安全防御的重要基础知识，也体现了 Web 安全防御方面的最新流行技术。重视实践是本书的第二大特点，书中展现了多个典型的攻防情景，再现了 Web 渗透的实际过程，让读者有身临其境之感，配合实战和实验讲解，能够保证读者技术能力的切实提高。由浅入深、循序渐进是本书的第三大特点，本书既给有经验的读者提供了精进技术的指导，也非常适合初学者快速掌握。

通过写序这个机会，也想告诉大家，读书不仅仅要学其中的知识，更重要的是透析作者的思路，灵活运用其中的各种技巧，梳理知识点，最终达到能够“讲书”的程度。

张胜生
工信部资深安全顾问
信息安全应急演练关键技术研究中心主任
东方宏宇国际咨询服务（北京）有限公司总经理

前　言

经过近 3 年时间的坚持和奋斗，终于将本书第 2 版完成。本书在第 1 版的基础上增加了大量内容，从 Web 渗透的专业角度系统探讨网络安全攻防技术，尽可能贴近实战，以帮助读者掌握本书的技术要点，再现 Web 渗透场景。

本书主要讨论 Web 渗透攻防技术。攻击与防护是辩证统一的关系，掌握了攻击技术，也就掌握了防护技术。Web 渗透是网络安全攻防的热门技术，攻击者可以通过渗透 Web 服务器，利用已有信息，逐渐深入公司或者大型网络，最终完成渗透。

近几年网络安全的相关话题特别火爆，可以说，从事网络安全是比较有“钱”途的职业之一。目前，各大安全公司都非常缺人，特别是在 CSDN、天涯、小米、Gmail、开心网、人人网等大型网站用户数据库泄露事件发生后，各大公司对安全人才求贤若渴——网站核心数据不安全，就失去了立足之本。掌握网络安全攻防技术、拥有丰富经验的从业人员年薪一般在 20 万元以上，能够独立挖掘漏洞的从业人员年薪一般在 30 万元以上。其实，Web 安全渗透技术也不是那么高不可攀，只要锁定方向，持之以恒，不断进行试验和研究，终将成为一名高手。而且，安全攻防技术与学历无关，很多技术高手都没有上过大学。

Web 渗透攻防技术可以通过以下方法自学：一是通过安全站点漏洞更新通告和安全文章了解漏洞的形成原理和利用过程，掌握漏洞的核心原理；二是在本地搭建试验环境进行实际测试，掌握漏洞的利用方法；三是在互联网上对存在漏洞的站点进行实际操作，在真实环境下进行验证，提出修补漏洞的方法。在研究技术的同时要做好记录，总结失败和成功的原因，积累技巧和经验。笔者曾经见过一位牛人，收集了超过 20GB 的 Web 漏洞数据！

本书内容

本书以 Web 渗透攻击与防御为主线，通过典型的渗透实例介绍 Web 渗透和防御技术，在每一节中，除了技术原理，还对这些技术进行总结和提炼。掌握和理解这些技术后，读者在遇到类似的渗透场景时可以自己进行渗透。本书采用最为通俗易懂的图文解说方式，按照书中的步骤即可还原攻防情景。通过阅读本书，初学者可以很快掌握 Web 攻防的流程及最新的技术和方法，有经验的读者可以在技术上更上一层楼，使攻防技术从理论和实践中更加系统化，同时，可以使用本书介绍的一些防御方法加固服务器系统。

本书共分 8 章，由浅入深，依照 Web 攻防的技术特点安排内容，每一节都是一个具体 Web 攻防技术的典型应用，同时，结合案例给予讲解，并给出一些经典的总结。本书主要内容安排如下。

第 1 章　Web 渗透必备技术

介绍 Web 渗透的基础知识，在 Windows XP 和 Windows 7 中创建及使用 VPN，域名查询技术，常用 DOS 基本命令，CX 端口转发实现内网突破，远程终端的安装与使用，Windows 下 PHP+MySQL

+IIS 安全试验平台的搭建，一句话后门的利用及操作，MySQL 数据库导入与导出攻略，以及 SQL Server 2005 还原数据库攻略等。这些技术可以在 Web 渗透中使用，也可以在网络管理中使用。

第 2 章　实战中常见的加密与解密

在 Web 渗透中经常会碰到数据被加密的情况，尤其是用户的密码，各个系统采用的密码加密算法不一样，如明文、MD5、SHA1、Base64 等。如果不了解常见的 Web 加密和解密方法，那么后续渗透工作将无法进行。本章主要介绍 Web 渗透过程中各种密码的破解及解密，获取和破解 Windows 及 Linux 操作系统密码的方法，以及绝大部分应用软件加密密码的获取和破解等。通过本章的学习，读者对后续渗透碰到的密码破解任务可以举一反三，触类旁通。

第 3 章　Web 漏洞扫描

Web 渗透技术的核心就是发现 Web 漏洞，我们可以通过扫描器进行漏洞扫描。本章主要介绍 Jsky、Acunetix Web Vulnerability Scanner、Safe3 等扫描工具，还对 Windows 操作系统、MSSQL、MySQL、FTP、路由器等的口令扫描和利用进行了介绍。

第 4 章　常见文件上传漏洞及利用

上传是 Web 渗透中最容易获得 WebShell 的途径之一。本章介绍了如何利用 WebEditor、FCKeditor、CuteEditor 等典型编辑器漏洞获取 WebShell 的方法，同时还对登录绕过后通过 Flash 上传、文件上传等方法获取 WebShell 进行了探讨。

第 5 章　SQL 注入漏洞及其利用

SQL 注入是 Web 渗透的核心技术。本章主要介绍如何使用 SQL 注入方法获取 WebShell，穿插介绍了如何使用多种扫描软件、攻击工具渗透 Web 服务器并提权。

第 6 章　高级渗透技术

本章介绍如何充分利用多种技术组合，结合巧妙的思路，最终成功渗透一些高难度的 Web 服务器，同时还对一些不常见的高级漏洞的利用进行了探讨。

第 7 章　Windows 和 Linux 提权技术

本章主要通过一些实例讨论如何进行 Windows 提权。这些提权方法比较经典，掌握这些提权方法后，对其他提权方法也可以触类旁通。Web 渗透的终极目标就是获取服务器权限，也即在获取 Webshell 权限后，利用现有信息和资源，通过各种途径，让 Webshell 权限提升到操作系统权限。Windows 提权的方法很多，本书仅介绍一些常见的提权方法，包括 MSSQL 和 MySQL 数据库提权、Serv-U 提权、Winmail 提权、Pr 提权、JBoss 提权。提权的核心思想就是通过应用程序或者操作系统漏洞，使普通用户获得 system 权限。

第 8 章　Windows 及 Linux 安全防范

本章就一些常见的漏洞和弱点进行分析，抛砖引玉。真正的安全防范是一个持续的改进和完善过程，需要随时关注 0day 及安全漏洞。在网络攻防的整个过程中，安全防范非常重要，攻击方需要隐藏自己的 IP 地址，消除痕迹，防止被发现，而防守方则关注如何加固，使自己的系统更加安全。

可以说，牢不可破是终极目标。在武侠小说中经常提及一个理念：最好的防御就是攻击。通过攻击自身系统发现漏洞，对漏洞进行分析、修补和加固，也就有了日常听到的安全公司进行某项目的安全评估。

虽然本书的内容已经比较丰富和完整，但仍无法涵盖所有的 Web 渗透技术。通过本书的学习，希望读者可以快速了解和掌握 Web 渗透技术，加固自己的服务器。本书的目的是通过 Web 渗透技术，结合一些案例探讨网络安全，从而更好地加固 Web 服务器，远离黑客的威胁。

资源下载

书中提到的所有相关资源可以到 http://www.antian365.com 下载，笔者在多年工作中收集的渗透工具包也免费供读者下载。

特别声明

本书的目的绝不是为那些怀有不良动机的人提供支持，也不承担因为技术被滥用所产生的连带责任。本书的目的在于最大限度地唤醒读者对网络安全的重视，并采取相应的安全措施，从而减少由网络安全带来的经济损失。

由于作者水平有限，加之时间仓促，书中疏漏之处在所难免，恳请广大读者批评指正。

反馈与提问

如果读者在阅读本书的过程中遇到任何问题或者对本书有任何意见，都可以直接发送邮件至 antian365@gmail.com 进行反馈。

致谢

感谢电子工业出版社对本书的大力支持，尤其是潘昕编辑为本书出版所做的大量工作，感谢美工对本书进行的精美设计。感谢多年来在信息安全领域给我教诲的所有良师益友，感谢众多热心网友对本书的支持。

感谢我的家人，是他们的支持和鼓励使本书得以顺利完成。

参加本书编写工作的有陈小兵、邓火英、庞香平、兰云碧、陈尚茂、杜鹏璐、孙立伟、林伟、杨卿、刘漩、范渊、冯国全、张茂荣、王玉莲、邱培东。另外，本书集中了 antian365 团队众多“小伙伴”的智慧。我们的团队是一个低调潜心研究技术的团队，在此衷心地向团队成员表示感谢，感谢雨人、imiyoo、cnbird、pt007、Mickey、Xnet、fido、指尖的秘密、Leoda、pt007、Mickey、YIXIN、终隐、fivestars、暖色调の微笑等，是你们给了我力量，给了我信念。

编　者

2015 年 4 月于北京

目　录