Broadview
www.broadview.com.cn

Web 安全攻防

渗透测试实战指南

徐焱　李文轩　王东亚　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 安全攻防

渗透测试实战指南

徐焱　李文轩　王东亚　著

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

内 容 简 介

本书由浅入深、全面、系统地介绍了当前流行的高危漏洞的攻击手段和防御方法，并力求语言通俗易懂，举例简单明了，便于读者阅读、领会。结合具体案例进行讲解，可以让读者身临其境，快速地了解和掌握主流的漏洞利用技术与渗透测试技巧。

阅读本书不要求读者具备渗透测试的相关背景，如有相关经验在理解时会更有帮助。本书亦可作为大专院校信息安全学科的教材。

图书在版编目（CIP）数据

Web 安全攻防：渗透测试实战指南 / 徐焱，李文轩，王东亚著. —北京：电子工业出版社，2018.7
ISBN 978-7-121-34283-7

Ⅰ. ①W… Ⅱ. ①徐… ②李… ③王… 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（2018）第 107744 号

策划编辑：郑柳洁
责任编辑：牛　勇
印　　刷：三河市君旺印务有限公司
装　　订：三河市君旺印务有限公司
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：787×980　1/16　印张：26　字数：464 千字
版　　次：2018 年 7 月第 1 版
印　　次：2018 年 8 月第 3 次印刷
定　　价：89.00 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）88254888，88258888。

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。

本书咨询联系方式：010-51260888-819，faq@phei.com.cn。

推荐序

经过老友夜以继日、逐字逐句地编写，本书终于出版了，在这里首先表示感谢，感谢编者将多年的工作经验汇聚成书。我从事信息安全工作已经18年，对于想从事渗透测试工作的朋友来说，我认为本书确实是一本难得的良师秘籍。我在阅读完本书后，和老友说，我会将本书推荐到北京中安国发信息技术研究院“全国5A级信息安全人才培养”的教材体系和“国家信息安全保障人员认证应急服务实践操作考试参考教材目录”中去，老友回复道，“本书涉及的实验将会很快推出，所有配套的实验将放到红黑演义网络安全学院的云端实验平台上供大家练习。”届时，读者可以一边阅读一边实践，实乃一大幸事！

我极力推荐专业从事渗透测试的人员、信息安全一线防护人员、网络安全厂商技术工程师、网络犯罪侦查与调查人员阅读本书，当然也推荐红黑演义网络安全院的2万名学员在想继续深造时学习本书配套的课程和实验。

具体的推荐理由有以下几点：

本书的实战性极强，比如在前期踩点阶段，“敏感信息收集”和“社会工程学”工作开展的细致程度就能体现出渗透者的阅历水平，如果这两方面的工作做好了，对后期提权和内网渗透的帮助就很大。

本书的进阶性好，实现了深入浅出地引导读者从入门到进阶，汇总了渗透测试工作中各种技术知识点的细微类型，渗透是否能够从里程碑直接到“黄龙府”，关键就在这些“细枝末节”上，我想这些地方对提高读者渗透水平的帮助应该是最大的。

本书对Web渗透技术原理的解读，透彻但不拖沓，对高效学习很有帮助，属于干货分享型。书中加入了大量绕过技术，这些技术在一些大型系统做了很多轮渗透之后再做渗透面临尴尬状态时特别有帮助。

本书介绍了一些在非常规渗透时用的技术和经验，比如“逻辑漏洞挖掘”“XXE

漏洞”，这样的漏洞利用哪怕是在知名的Facebook、PayPal等网站上都引发过问题。尽管XXE漏洞已经存在了很多年，但是从来没有获得它应得的关注度。很多XML的解析器默认是含有XXE漏洞的，这意味着渗透测试人员应该去测试、验证它。

最后，本书还给出了常用工具和各式利器，并详细讲解了使用它们的技巧和步骤，这些工具会大大降低渗透测试人员的劳动强度，快速将客户的系统漏洞挖掘出来。

张胜生　2018 年 4 月 12 日于北京
北京中安国发信息技术研究院院长
工信部/教育部网络安全领域专家
省级产业教授/研究生导师
北京市级百名网络安全专家负责人
CISSP认证考试指南译者/资深讲师
中国信息安全认证中心应急服务人员认证体系牵头人

前言

对于网络安全专业的人士来说，2017年是忙碌的一年，我们经历了美国国家安全局的敏感数据泄露事件、各种“邮件门”事件、“想哭”（WannaCry）勒索病毒肆虐全球，以及“8·19徐玉玉电信诈骗案”等安全大事。随着智能终端改变着人们生活中的方方面面，互联网渗透进国民经济的各行各业，用户的隐私安全受到更大威胁，企业也面临着向互联网企业的转型和升级，信息安全将成为未来所有普通人最关心的问题之一。

随着“网络空间安全”被批准为国家一级学科，各高校网络空间安全学院如雨后春笋般纷纷成立，但各高校的网络安全教育普遍存在一个问题，便是很少全面、系统地开设“渗透测试”方面的课程，而“渗透测试”作为主动防御的一种关键手段，对评估网络系统安全防护及措施至关重要，因为只有发现问题才能及时终止并预防潜在的安全风险。目前市面上的网络安全书籍良莠不齐，希望本书能为网络安全行业贡献一份微薄之力。

本书出版的同时计划出版姐妹篇——《内网安全攻防：渗透测试实战指南》，目前已经在撰写中，具体目录及进展情况可以在http://www.ms08067.com中查看。

本书结构

本书基本囊括了目前所有流行的高危漏洞的原理、攻击手段和防御手段，并结合大量的图文解说，可以使初学者很快掌握Web渗透技术的具体方法和流程，帮助初学者从零开始建立起一些基本技能。

全书按照从简单到复杂、从基础到进阶的顺序讲解，不涉及一些学术性、纯理论性的内容，所讲述的渗透技术都是干货。读者按照书中所讲述的步骤操作即可还原实际的渗透攻击场景。

第 1 章　渗透测试之信息收集

进行渗透测试之前，最重要的一步就是信息收集。在这个阶段，我们要尽可能地收集目标的信息。所谓“知己知彼，百战不殆”，我们越了解测试目标，测试的工作就越容易。本章主要介绍了域名及子域名信息收集、查找真实IP、CMS指纹识别、目标网站真实IP、常用端口的信息收集等内容。

第 2 章　搭建漏洞环境及实战

“白帽子”在目标对象不知情或者没有得到授权的情况下发起的渗透攻击是非法行为，所以我们通常会搭建一个有漏洞的Web应用程序，以此来练习各种各样的安全渗透技术。本章主要介绍了Linux系统下的LANMP、Windows系统下的WAMP应用环境的搭建，DVWA漏洞平台、SQL注入平台、XSS测试平台等常用渗透测试漏洞练习平台的安装配置及实战。

第 3 章　常用的渗透测试工具

“工欲善其事，必先利其器”，在日常的渗透测试中，借助一些工具，“白帽子”可以更高效地执行安全测试，这能极大地提高工作的效率和成功率。本章详细介绍了常用的三大渗透测试工具SQLMap、Burp Suite、Nmap的安装、入门和实战利用。

第 4 章　Web 安全原理剖析

Web渗透的核心技术包括SQL注入、XSS攻击、CSRF攻击、SSRF攻击、暴力破解、文件上传、命令执行漏洞攻击、逻辑漏洞攻击、XXE漏洞攻击和WAF绕过等。本章依次将这些常见高危漏洞提取出来，从原理到利用，从攻击到防御，一一讲解。

同时还讲解了CSRF漏洞、SSRF漏洞、XXE漏洞、暴力破解漏洞、命令执行漏洞、文件上传漏洞、逻辑漏洞的形成原理、漏洞利用、代码分析，以及修复建议。

第 5 章　Metasploit 技术

Metasploit是近年来最强大、最流行和最有发展前途的开源渗透测试平台软件之一。它完全颠覆了已有的渗透测试方式。本章详细介绍了Metasploit的攻击步骤、信息收集、漏洞分析、漏洞利用、权限提升、移植漏洞代码模块，以及如何建立后门的实践方法。通过具体的内网域渗透测试实例，分析如何通过一个普通的WebShell

权限一步一步获取域管权限，最终畅游整个内网。

第 6 章　PowerShell 攻击指南

在渗透测试中，PowerShell是不能忽略的一个环节，而且仍在不断地更新和发展，它具有令人难以置信的灵活性和功能化管理Windows系统的能力。PowerShell的众多特点使得它在获得和保持对系统的访问权限时，也成为攻击者首选的攻击手段。本章详细介绍了PowerShell的基本概念和常用命令，以及PowerSploit、Empire、Nishang等常用PowerShell攻击工具的安装及具体模块的使用，包括生成木马、信息探测、权限提升、横向渗透、凭证窃取、键盘记录、后门持久化等操作。

第 7 章　实例分析

对网站进行渗透测试前，如果发现网站使用的程序是开源的CMS，测试人员一般会在互联网上搜索该CMS已公开的漏洞，然后尝试利用公开的漏洞进行测试。由于CMS已开源，所以可以将源码下载，直接进行代码审计，寻找源码中的安全漏洞。本章结合实际的源码，详细介绍了如何找出SQL注入漏洞、文件删除漏洞、文件上传漏洞、添加管理员漏洞、竞争条件漏洞等几种常见安全漏洞的代码审查方法，并通过实际案例细致地讲解了几种典型的攻击手段，如后台爆破、SSRF+Redis获得WebShell、旁站攻击、重置密码攻击和SQL注入攻击，完美复现了整个实际渗透攻击的过程。

特别声明

本书仅限于讨论网络安全技术，书中展示的案例只是为了读者更好地理解攻击者的思路和操作，以达到防范信息泄露、保护信息安全的目的，请勿用于非法用途！

严禁利用本书所提到的漏洞和技术进行非法攻击，否则后果自负，本人和出版商不承担任何责任！

联系作者

读者在阅读本书过程中遇到任何问题或者有任何意见，都可以直接发电子邮件至8946723@qq.com进行反馈。

读者也可以加入本书的交流QQ群（736151662）进行交流。

同步网站内容

本书的同步网站为http://www.ms08067.com，该网站主要提供以下资源。

- 本书列出的一些脚本的源代码。
- 本书讨论的所有工具和其他资源的下载或链接。
- 关于本书内容的勘误更新。

读者服务

轻松注册成为博文视点社区用户（www.broadview.com.cn），扫码直达本书页面。

- **提交勘误**：您对书中内容的修改意见可在 提交勘误 处提交，若被采纳，将获赠博文视点社区积分（在您购买电子书时，积分可用来抵扣相应金额）。
- **交流互动**：在页面下方 读者评论 处留下您的疑问或观点，与我们和其他读者一同学习交流。

页面入口：http://www.broadview.com.cn/34283

致谢

感谢电子工业出版社编辑吴倩雪审阅本书稿，找出了书中的许多错误。感谢我的兄弟徐儒弟对本书封面的精美设计。感谢李韩对本书同步网站的精心制作。

感谢carry_your、武鑫、张苗苗、椰树、TT参与了本书部分内容的编写。感谢张胜生、陈亮、程冲、周培源、周勇林、Mcvoodoo、尹毅百忙之中抽空为本书写序、

写推荐语。

感谢各位圈内的朋友，他们包括但不限于：陈小兵、矩阵、klion、key、不许联想、暗夜还差很远、博雅、杨凡、曲云杰、陈建航、位面消隐、Demon……

感谢我的父母，感谢你们含辛茹苦地将我抚育成人，教会我做人的道理，在我生命的任何时刻都默默地站在我的身后，支持我，鼓励我！

感谢我的妻子，撰写本书基本占用了我所有的业余时间，几年来，感谢你每天在忙碌的工作之余对我的照顾和呵护。谢谢你为我付出的一切，你的支持是对我最大的鼓励。

感谢徐晞溪小朋友，你的到来让爸爸的世界充满了阳光，家里每个角落都充满了你咯咯咯的笑声。希望你可以慢些长大，你永远在爸爸内心最柔软的地方！

最后，感谢那些曾在我生命中经过的你们，感谢你们曾经的陪伴、帮助和关爱，这些都是我生命中不可或缺的一部分，谢谢你们！

念念不忘，必有回响！

徐焱

2018年4月于镇江

目录