Broadview
www.broadview.com.cn

安全技术大系

Web渗透技术及实战案例解析

陈小兵 范渊 孙立伟 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

Web渗透技术及实战案例解析

陈小兵 范渊 孙立伟 编著

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

内 容 简 介

本书从 Web 渗透的专业角度，结合网络安全中的实际案例，图文并茂地再现 Web 渗透的精彩过程。本书共分 7 章，由浅入深地介绍和分析了目前网络流行的 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对应的安全防范措施，对一些经典案例还给出了经验总结和技巧，通过阅读本书可以快速掌握目前 Web 渗透的主流技术。本书最大的特色就是实用和实战性强，思维灵活。内容主要包括 Web 渗透必备技术、Google 黑客技术、文件上传渗透技术、SQL 注入、高级渗透技术、0day 攻击和 Windows 提权与安全防范等。

本书内容丰富，深入浅出，图文并茂，可供对网络安全感兴趣的读者使用，同时也适合作为计算机应用专业高年级本科生和研究生的网络安全课程实践参考资料。

图书在版编目（CIP）数据

Web 渗透技术及实战案例解析 / 陈小兵，范渊，孙立伟编著. —北京：电子工业出版社，2012.4
（安全技术大系）
ISBN 978-7-121-16181-0

Ⅰ. ①W… Ⅱ. ①陈… ②范… ③孙… 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(2012)第 039567 号

策划编辑：毕　宁　　bn@phei.com.cn
责任编辑：徐津平
特约编辑：顾慧芳
印　　刷：北京丰源印刷厂
装　　订：三河市鹏成印业有限公司
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：44.75　字数：1088 千字
印　　次：2012 年 4 月第 1 次印刷
印　　数：4000 册　　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。

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。

前　言

经过近一年时间的艰辛苦战，终于将本书完成。本书是我写的第三本书，主要从 Web 渗透的专业角度来讨论网络安全的攻防技术，尽可能地再现 Web 渗透场景，每一个小节都代表某一个场景，此书是我工作数年的总结，最后终于不辱使命将所有成果放在本书中与大家分享。

本书是在我上一本书《黑客攻防及实战案例解析》基础上的又一本安全类书籍，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最热门技术，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，最终完成渗透目标。

最近二年来网络安全特别火爆，可以说从事网络安全还是蛮有前途的职业之一。目前网络安全界非常缺人，特别是在 2011 年 CSDN、天涯等大型网站用户数据库泄露后，各大公司对安全人士求贤若渴，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 10 万以上，能够独立挖掘漏洞的从业人员年薪一般在 20 万以上。其实 Web 安全渗透技术也不是那么高不可攀，只要自己锁定这个方向，持之以恒，不断地进行试验和研究，终将成为一名高手，而且安全攻防技术还跟学历无关，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来自学，一是通过安全站点漏洞更新通告、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。在技术研究的同时还要做好记录，总结失败和成功的方法，积累技巧和经验，我曾经看过一位牛人，Web 漏洞收集超过 10GB 数据！

本书以 Web 渗透攻击与防御为主线，主要通过典型的渗透实际案例来介绍 Web 渗透和防御技术，在每一个小节中除了技术原理外，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去进行渗透。本书采用最为通俗易懂的图文解说，按照书中的步骤即可还原当时的攻防情景。通过阅读本书，初学者可以很快掌握 Web 攻防的流程、最新的一些技术和方法，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，同时可以使用本书中介绍的一些防御方法来加固服务器系统。

本书共分为 7 章，由浅入深，依照 Web 攻防的一些技术特点安排内容，每一小节都是一个具体 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 渗透的一些必备的基本知识，创建和使用 VPN 隐藏自己，获取操作系统密码、破解 MD5 密码、破解 MySQL 密码、数据库还原等，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 Google——我爱你又恨你

利用 Google 等搜索引擎技术来获取信息，辅助 Web 渗透，在某些场景中往往会起到意想不到的效果，也被称为 Nday 攻击（0day 后的数天持续攻击）。在进行 Web 攻防技术研究的同时，可以通过 Google 来进行实际演练，最好的效果就是网上爆出漏洞后利用 Goolge 技术来抓肉鸡。

第 3 章 都是上传惹的祸

上传是 Web 渗透中最容易获得 WebShell 的捷径之一，在本章中介绍了如何利用 WebEditor、FCKeditor、CuteEditor 等典型编辑器漏洞来获取 WebShell 的方法，同时还对登录绕过后通过 Flash 上传、文件上传等方法来获取 WebShell 进行探讨。

第 4 章 SQL 注入——渗透主乐章

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

第 5 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。

第 6 章 0day 攻击

0day 是 Web 渗透中的“神器”，几乎是无往不胜，所向披靡，本章介绍利用 Discuz!6.0、Discuz!7.2、Discuz!NT、PHP168、WordPress、Citrix、Art2008cms、Phpcms2008sp4 等 0day 渗透 Web 服务器的一些方法。

第 7 章 Windows 提权与安全防范

获取 WebShell 后，获得服务器权限一直是 Web 渗透的终极目标，本章对主流的一些提权方法进行介绍，掌握这些方法和原理后，可以举一反三，触类旁通。最后还对如何设置一个安全“变态”的 Web 服务器进行介绍。

虽然本书内容已经很丰富与完整，但仍然无法涵盖所有的 Web 渗透的技术，但通过本书的学习，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 渗透技术并结合一些案例来探讨网络安全，更好地加固 Web 服务器、远离黑客的威胁。

资源下载

笔者在书中提到的所有相关资源可以到 http://www.antian365.com 下载。

特别声明

本书的目的决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大家对网络安全的重视，并采取相应的安全措施，从而减少由网络安全而带来的经济损失。

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

读者在阅读本书过程中所遇到任何问题或者意见，可以直接发邮件至 simeon@antian365.com，也可去我个人 Blog（http://simeon.blog.51cto.com）留言。

致谢

感谢电子工业出版社对本书的大力支持，尤其是毕宁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的设计。借此机会，我还要感谢多年来在信息安全领域给我教诲的所有良师益友，感谢众多热心网友以及 51cto 技术好友等对本书的支持。最后感谢我的家人，是他们的支持和鼓励使得本书得以顺利完成。

另外，本书集中了安天 365 团队的智慧，我们团队是一个低调潜心研究技术的团队，我衷心地向团队表示感谢，是你们给了我力量，给了我信念，他们主要是 cnbird、Xnet、指间的秘密、网络蜘蛛侠、BlAck.Eagle、COEED1F3、lovec、上帝之爱、Leoda、kiss、陆羽、oldjun、暮云飞、fjhh、藏形匿影、啊乖、pt007、FF@F.S.T、花非花、花生、Mickey、余弦、玉鼎真人、雕牌卫生巾、Frank.c、石头、robert、ラ林ぜ等。

编　者

2011 年 10 月于北京

目　录