Broadview
www.broadview.com.cn

安全技术大系

Web前端黑客技术揭秘

钟晨鸣 徐少培
编著

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

Web前端黑客技术揭秘

钟晨鸣 徐少培
编著

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

内 容 简 介

Web 前端的黑客攻防技术是一门非常新颖且有趣的黑客技术，主要包含 Web 前端安全的跨站脚本（XSS）、跨站请求伪造（CSRF）、界面操作劫持这三大类，涉及的知识点涵盖信任与信任关系、Cookie 安全、Flash 安全、DOM 渲染、字符集、跨域、原生态攻击、高级钓鱼、蠕虫思想等，这些都是研究前端安全的人必备的知识点。本书作者深入剖析了许多经典的攻防技巧，并给出了许多独到的安全见解。

本书适合前端工程师阅读，同时也适合对 Web 前端各类安全问题或黑客攻防过程充满好奇的读者阅读，书中的内容可以让读者重新认识到 Web 的危险，并知道该如何去保护自己以免受黑客的攻击。

图书在版编目（CIP）数据

Web 前端黑客技术揭秘 / 钟晨鸣，徐少培编著. —北京：电子工业出版社，2013.1
（安全技术大系）
ISBN 978-7-121-19203-6

Ⅰ. ①W… Ⅱ. ①钟… ②徐… 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 295360 号

策划编辑：毕 宁
责任编辑：李利健
印 刷：中国电影出版社印刷厂
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：787×980 1/16 印张：23.75 字数：608 千字
印 次：2013 年 1 月第 1 次印刷
印 数：4000 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。

序 1

有人说互联网是由人组成的，也有人说互联网是由代码组成的。如果说互联网是由代码组成的，那么 Web 前端代码占据着互联网至少半壁江山；如果说互联网是由人组成的，那么有人的地方就有江湖，江湖中总是有剑客高手，互联网中也总是有技术黑客高手。

剑客也好，黑客也好，他们总是用各种让人叹为观止的奇妙招数让人在还未反应过来时就已经中招。一个人要在江湖中畅意行走，就要会点武功。同理，要在互联网上快意冲浪，就需要了解黑客的知识。只有做到知己知彼，才能“笑傲江湖”。

非常感谢钟晨鸣邀请我写这个序言，钟晨鸣是少有的理论+实战的天才型“黑客”，我非常佩服他在 Web 安全方面的造诣。更难能可贵的是，他和徐少培将自己的知识精华毫无保留地整理出来，写成“剑谱”公诸于世。“练练武功”不但可以防身，更能强身健体，这本书是我看到他们一路写成的，前后用了一年多的时间，花费了无数心血，写得非常细致，我预先读了本书，不敢独藏，与君共享。

顺便提一下，当前 Web 2.0 和 HTML5 已经渗透到了互联网及我们生活的方方面面，例如：

- 腾讯的 Q+和 Web QQ 上拥有近 10 万个 Web 应用。
- Google 的 Chrome 网上应用商店提供了 7 万多个应用，拥有数亿人次的应用用户。
- 4399.com 拥有数万个在线网页游戏。
- 安卓和苹果上当前 17%的应用都是使用 HTML 5 开发的，而且这个比例还在不断上升。

- SAAS 的普及，使大量网站应用服务于我们的方方面面。

……

可以说，未来的互联网在很大程度上将由 HTML+JavaScript+CSS 构成，而安全是互联网发展的基础，互联网安全将在很大程度上取决于 Web 前端安全，如果前端失陷，我们的个人隐私、在线支付信息等都将受到莫大的挑战。

本书非常系统地讲解了 Web 相关的安全问题，图文并茂，理论和实战面面俱到，而且非常难得的是，书中有很多意想不到的“黑客”思路，这些思路非常具有实战性和前瞻性。

如果你是开发人员，保护客户的隐私是第一天职，那么看看这本书吧，它能教你如何编写安全的应用。

如果你是普通网民，要保障自己的安全，需要看看我们都面临什么挑战，那么看看这本书吧，它能让你明白平常应该注意什么。

如果你是善意的黑客，想换换思路，看看这本书吧，它能给你意想不到的视角和思路。

知道创宇 CTO　杨冀龙

2012 年 10 月 8 日

序 2

网络安全永远伴随着业务的变化而变化。十几年前，互联网的兴起把 Web 服务推到了浪潮之巅。从此步入 Web 1.0 时代，伴随 Web 业务而来的 Web 安全也逐渐兴起，Web 1.0 时代的安全主要体现在服务端动态脚本及 Web 服务器的安全问题上。到了 2004 年，Web 2.0 的诞生标志着又一次互联网革命到来！而这个时候的 Web 安全随着 2005 年由当时年仅 19 岁的天才 Samy Kamkar 在 MySpace 上爆发了历史上第一个 XSS Worm 震惊了整个世界，由此也宣告 Web 安全正式步入 Web 2.0 时代。这个时代的安全关注点已经由服务端全面转向了客户（前）端，浏览器替换 Web 服务器成为安全战争的主要战场，而前端常用的 HTML、JavaScript、CSS、Flash 等则成为安全战场的有力武器，浏览器挂马、XSS、CSRF、ClickJacking 等成了主流的攻击手段。有攻击就有防御，面对 Web 2.0 时代的安全问题，Web 1.0 时代的防御体系显得力不从心，很多安全从业者们都在思考和尝试新的防御手段，一场基于前端黑客攻防战就此拉开序幕……

作为一名资深的“脚本小子”，我有幸经历了 Web 安全由 Web 1.0 向 Web 2.0 转变的整个过程，也目睹了很多致力于 Web 2.0 安全技术研究的公司诞生及发展的过程，并结识了一大群优秀的 Web 安全研究者，其中就有本书的两位作者：钟晨鸣先生和徐少培先生。

认识钟晨鸣先生缘于他所在的北京知道创宇信息技术有限公司。该公司于 2007 年成立，是国内最早关注 Web 2.0 时代安全防御的公司之一，并在 Web 2.0 安全防御领域里取得了巨大的成绩。而钟晨鸣先生早在 2008 年就加入了该公司，并积极加入到 Web 2.0 的各种攻防技术研究中，后来逐步成为公司技术的中流砥柱。也是在这些官方对抗的实战中，成

就了他对 Web 2.0 时代安全技术的独特认识，并逐步完善了自己的技术体系。

而徐少培先生所在的北京天融信科技有限公司，是一家经历了 Web 1.0 时代的传统的信息安全公司，随着 Web 2.0 时代的安全挑战，也使他们的研究人员投身于这个领域，由此培养了一大批技术精湛的安全研究者。徐少培先生就是其中之一，他对 Web 2.0 安全技术有着深入的研究，尤其是在 HTML 5 的安全领域，他一直处于领先的地位。

如果说技术积累是本书诞生的“硬件”基础，那么乐于分享的精神就是本书诞生的必要的“软件”基础。有幸的是，钟晨鸣先生和徐少培先生都具有这样的分享精神，他们一直在通过 Blog 及参加各种技术峰会等不断分享着他们的研究成果。

所以，本书的诞生是他们对技术研究的总结及乐于分享精神的结合的成果。而我有幸成了该书的第一位读者，接到这本书的时候，我很惊讶，因为写书在我看来是一件很“痛苦”的事情。另外，对于 Web 2.0 安全技术题材的书，在中国图书市场上是不多见的，纯技术分享的书籍更是寥寥无几，而他们的尝试显然是成功的！

本书是一本纯技术的关于 Web 2.0 时代安全的专业书籍，从浏览器战场到前端的各种武器及攻击手段，再转到防御技术，都做了专业详细的展示。最后，我要说的只有一句话：本书值得您期待！

superhei

2012 年 10 月 18 日

前　言

安全之路任重道远，前端安全是众多安全中的一个分支，互联网上各种网站让人眼花，千奇百怪的业务需求、安全问题，真要做好安全架构又谈何容易呢？我们知道，这次我们仅仅为互联网安全的进化奠定了一块砖头而已。

本书点透了很多关键的点，每个点的内容不一定覆盖完全，也不一定用了足够的文字进行描述，往往适可而止，但这些点却是 Web 前端安全基石的重要组成，如：信任与信任关系、Cookie 安全、Flash 安全、DOM 渲染、字符集、跨域、原生态攻击、高级钓鱼、蠕虫思想等。

我们试图尽最大的努力使本书的内容涵盖完全，但发现这是不可能的事。闻道有先后，术业有专攻，我们写出了我们擅长的点，还有很多点是我们不敢去写的，时间与精力是我们最大的障碍。另外，我们认为，本书的知识点足以打开 Web 前端黑客的大门，有了这些沉淀后，大家完全可以持续跟进国内外优秀的技术文章与案例进行内功修炼，并在各种实战中不断加强。

网站安全是一个大问题，安全关注点也在逐渐转移，从刚开始的服务端安全，如缓冲区溢出、CGI 解析缺陷、纯 Web 层面的 SQL 注入等，到客户端安全，如 XSS 跨站脚本、CSRF 跨站请求伪造等。大家的意识与防御层面也随着 Web 安全的发展进化着。对网站来说，重视某些安全风险最好的办法就是将该风险最大化，这也是本书的目的，最终是让 Web 更好、更安全。

■ 一些约定

- 本书说的前端都指 Web 前端，也可以说是客户端，或者浏览器端。
- 本书涉及的前端安全舞台基本上都是浏览器。浏览器更新换代的速度非常快，也许在你看到本书时，一些技巧已经不适用了。没关系，因为思想更重要，我们在撰写本书时默认使用的主流浏览器的最新版本是：Firefox 15、Chrome 21、IE 9。

■ 前端黑客的内容

前端安全主要有三类：XSS、CSRF、界面操作劫持。从 XSS 到 CSRF，再到界面操作劫持，越往后，社工（社会工程学的简称）成分越浓厚。我们会发现这个 Web 世界越不可信，攻击也似乎变得越无聊，实施这类攻击的代价也越来越大。界面操作劫持需要很好的美工基础，因此，你让一个黑客去搞美工是不太现实的，因为现在有很多好的方式可以黑下目标。

所以，本书关于界面操作劫持的内容更多的是具有研究性质的，而很少用于真正的攻击，即使我们已经完成了一些很有意义的攻击事件（比如，针对 Google Reader 的蠕虫事件），但都是善意的，在真正的黑客攻击活动中，这样做的可能性很小。

有一点我们都应该明白，当前还不具备“黑客攻击活动”价值的风险，以后可能会具备，回头看看整个安全发展史就可以发现这个规律。至少 XSS 与 CSRF 已经具备这样的价值，而且发展得如火如荼。这也是本书的重点内容。

■ 为什么进行前端黑客研究

Web 从 Web 1.0 到 Web 2.0，一个用户参与度与黏性都很高的 Web 时代，且 Web 2.0 又细分出许多不同的领域（微博、旅游、交友、餐饮、医疗、购物等），各种海量的隐私数据可以在这些 Web 2.0 网站中找到。前端黑客是随着这个趋势发展起来的，通过前端黑客

技巧，往往很容易就掌控了目标用户的隐私数据。

另外，攻击时获取各种隐私数据或者破坏数据，其实很多时候都可以在前端攻击中完成，而且目前看来由于安全意识的问题，很多安全焦点都还在服务端，比如，OS（操作系统）加固得如何、数据库加固得如何、SQL 查询是否参数化了、是不是存在弱口令等。那么，前端安全就被忽略了，在某些场景中，前端漏洞，比如一个 XSS 漏洞的价值就很大，而且前端攻击同样也可以大规模地进行，造成很大的影响。

我们在很多次的实战中运用了前端黑客技术，这是一种具备实战意义的技术，非常值得大家深入了解。

前端黑客技术的研究是一种趋势，它已经成形了，这就是我们为什么要介绍前端黑客的原因，也是本书诞生的最根本原因。

■ 阅读指南

本书共 10 章，每章的关联性不强，大家可以根据自己的喜好跳跃性地阅读，不过我们建议从头到尾地阅读，因为每章的信息量都比较大，我们没法完全照顾初学者，很多更基础的知识点需要自己去弥补。

第 1 章介绍 Web 安全的几个关键点。这些关键点是我们研究前端安全的意识点，缺乏这些关键意识，就很难真正弄懂前端安全，本章的内容值得细细阅读。

第 2 章介绍前端基础。实际上，其中的很多内容并非真正的基础，本书不会像传统的教材那样回顾那些语言的语法、用法等，我们会从安全的角度出发，介绍前端角色（URL、HTTP、HTML、JavaScript、CSS、ActionScript 等）的行为，以此来理解做前端安全都需要具备哪些基本技能，我们觉得基础是关键，所以本章内容会比较多。

第 3 章介绍前端黑客之 XSS，第 4 章介绍前端黑客之 CSRF，第 5 章介绍前端黑客之界面操作劫持，这几章的内容都不多，但却是理解 XSS、CSRF、界面操作劫持的关键，为更好地理解后面的章节打好基础。

第 6 章介绍漏洞挖掘。这是难度非常大的部分，我们不可能涵盖完全，甚至有些知识点我们都无法详细介绍，只是尽可能地将我们的经验与大家分享，其中涉及很多漏洞挖掘思想与技巧，需要大家仔细理解，同时希望大家能够举一反三，激发出更多的挖掘思路。

第 7 章介绍漏洞利用。有了前面的知识后，我们又面对一个高难度的过程，这是前端黑客渗透实战的关键步骤。本章给出了很多经典的攻击向量，并剖析了多个真实案例。

第 8 章介绍 HTML5 安全。这是一个很火热的概念，虽然我们在前面章节中提到了 HTML 5 安全，不过还是有必要用单独一章将更多的内容集中展现出来。

第 9 章介绍 Web 蠕虫。实际上就是 Web 2.0 里发生的蠕虫攻击，包括 XSS 蠕虫、CSRF 蠕虫、ClickJacking 蠕虫等，其中的案例都很经典，这基本属于前端黑客攻击的中级篇，而高级篇属于某些真正的前端黑客渗透实战。

第 10 章介绍关于防御。黑客不是专搞攻击的，在之前的一些章节中，我们在介绍攻击时，有必要也会提到防御，同时我们专门在本章从三个角度出发（浏览器厂商、Web 厂商、用户），给出了更多的防御建议，作为全书的终结。

作　　者

特别说明：我们计划上线 web2hack.org，定位：Web 前端黑客相关资源与观点的分享，请大家关注。

致　　谢

我要感谢的人太多。

首先要感谢我老婆的大力支持，如果不是她，这本书的问世也许会更晚。她舍弃了很多本该休闲游玩的时间陪着我，目的就是让我能专心写完此书，我承诺我会爱她一辈子，多陪她，这本书献给她。

感谢我父母的关爱，他们从来不会索取任何回报，我希望他们以我为荣。

感谢本书的第二作者 xisigr，他说我感染了他，让他有了巨大的激情。而我认为是他感染了我，要不是他，本书很难问世，他是一个做事认真，又喜欢养各种奇怪小动物的人，他虽然身在传统安全厂商，但却有一颗做互联网的心。

感谢 monyer 为本书的混淆代码添加了各种好料，他是一名难得一见的高效率、高智商的实战黑客。

感谢 XEYE 团队的其他成员，他们很低调，名字都不让我提，但是熟悉的人都认识他们，他们是一群可爱的人，能和他们结交是我的幸运，我们每次相聚总有一种亲切感，这是一个难得的团队。

感谢我所在的知道创宇安全研究团队，他们给了我很多的支持与灵感，他们在做着 Web 安全领域很酷的事情，大家可以感受到他们的分享精神。

感谢黑哥（网名：superhei）为本书提供了大量建议与错误指正。黑哥是一位让我由衷欣赏的人，他的身上体现出了那种亦正亦邪的黑客精神，这种精神的感染力很大。他说，如果他写这本书，就完全不是这样的风格，所以，大家如果要了解更多，看他的博客去吧，或者结交他。

感谢毕宁，没有他的帮助，根本不会有这本书，很荣幸，他现在与我共事了，我们在知道创宇公司工作，他是一位值得结交的豪爽之人。

感谢 soglili（李普君），这个小孩的思维与常人不同，是一个非常聪明的人，他喜欢无约束地做事，他为本书贡献了许多混淆代码。

感谢那些为本书添砖加瓦的人，还有微博、QQ 群里以及身边那些支持我的朋友们，以及为 Web 前端安全发展做出各种贡献的跨站师们，本书的很多灵感来源于他们。

最后要感谢我的公司知道创宇，我在 2008 年毕业前就跟随公司一起创业到现在，当时的几位前辈给了我很多指点。公司从几人小团队到现在初具规模，我们一直往我们的使命奔跑前进，我们天生具备大数据处理的基因。为了生存，我们在传统的安全市场上和竞争对手抢江山，现在我们又在互联网上攻城略地，一个还不大的团队做了很多事，因为我们的愿景是让互联网更好、更安全，我们会一直努力下去。

时间对我来说非常宝贵，我只能用我的业余时间把我们所知的写出来，与大家共享，如果有错误的地方，还希望各位不吝赐教。

第一作者　钟晨鸣（网名：余弦）

我于 2008 年加入天融信阿尔法实验室，同年加入了 XEYE 团队。时至今日，每逢 XEYE 聚会，我们都会聊起各自加入 XEYE 时的趣闻轶事。写书也是在聚会上说起的，印象中应

该是 2009 年冬天在好伦哥聚餐……而开始动笔去写已是 2011 年 3 月。如今，书已经定稿了。细数上面我提及的几个日期数字，真是白驹过隙。

我要把这本书奉献给我挚爱的妻子，因为见到她第一眼时，我不知道现在她对我如此重要。

感谢我的父母时常在电话里给予我的鼓励。感谢余弦提供的这个机会，使我可以为本书执笔，这些年他一直是我的良师益友。

最后要感谢天融信阿尔法实验室自由的优越的工作氛围，那里赋予我更多独立思考的空间。

最后我想说的是，这本书倾尽了我们的心血，在引领读者走进 Web 前端安全的同时，如果还能有幸提升 Web 安全界的整体水平，那我们将感到无比荣耀。

第二作者　徐少培（网名：xisigr）

目　录