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，它已经成型了，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