

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