<<黑客WEB脚本攻击与防御技术 >

图书基本信息

书名：<<黑客WEB脚本攻击与防御技术核心剖析>>

13位ISBN编号：9787030260116

10位ISBN编号：7030260112

出版时间：2010-1

出版时间：科学出版社

作者：郝永清

页数：360

字数：563000

前言

本着序的第一要义：坦率、诚实、中肯，对读者负责，对社会负责而作此序。
网络安全技术在中国，更多的是神秘化、妖魔化。
如果将外界加诸于网络安全技术身上的浮华外表剥去，剩下的和一群车间技术工人绞尽脑汁的研究、突破某个生产设备运行瓶颈的行为毫无区别：网络安全技术只是一种技术进步过程中必然存在的推动力而已，只是这种推动力必须要破开层层桎梏，以至于在冲击的过程中无意间影响了立场不坚定者、心底阴暗者或利欲熏心者。
当本书责编田sir与我提及要系统的编著一套网络安全技术的相关书籍，能否为之作序的时候，我考虑的并不是究竟什么技术应该普及？
什么技术应该得到大家的重视？
什么技术到目前还没有达到公布并讨论的临界点？
我考虑最多的其实是一个和本书的编者、读者一样，一个可能被不了解的人冠以“ 黑客 ”这个原本崇高现在却遭人唾弃的中国网络安全圈中的参与者的社会责任感。
网络安全参与者的社会责任感是什么？
无外乎参与者们对国家、集体、他人所承担的职责、任务和使命的正面积极的态度。
怀揣着这样的责任感再来通读本书，或许读者能和我一样，在字里行间的技术之外，发现一些作者细微但却真挚的责任感——是的，作者和我们拥有的一样的正面积极的责任感。
正是这样的责任感，让作者在编著此书时，选取题材的时候并没有和其他同类书一样，为求眼前利益而一味的选择破坏却舍弃建设、突出攻击却忽略防御、细致利用而敷衍维护。
虽然作者选取的题材是未来一段时间必将成为网络安全重点的Web服务方面的攻防技术，但是作者在这些新技术的普及过程中，不忘技术探讨的本质，不忘攻防一体的方式，不忘对读者的网络安全思维方式进行力所能及的正确导向，这是难能可贵的。
从内容选择上说，作者很别致地选取了目前具有一定热度的相关技术进行常规普及，但是重点放在具有前瞻意义的新技术讨论上。
稍微对网络安全技术发展过程有所了解的人，基本看法应该都和作者一样：基于Web服务方面的攻防技术无疑是现在的网络安全的重点内容。
其中脚本（数据库）注入、cookies攻防都是现在攻击者们最喜欢利用的手法，也都是战斗在第一线的网络安全工程师们每天需要面对的问题。

内容概要

网络的发展是当今世界最大的变革，随网络普及带来的网络信息安全也成为全世界共同关注的热点话题。
在世界范围内，关注人数最多、技术实用性最高、破坏力最强、防护难度最高的黑客攻击技术非Web脚本攻击莫属——这也是本书的主题。
本书以网络安全技术中时下最火爆的Web脚本攻击为主要讲解方向，以实例分析加案例剖解为主要脉络，以作者逾8年的网络安全技术实际经验为借鉴，以藏锋者网络安全网(www.cangfengzhe.com)会员关注热点为基础，以图文并茂、按图索骥的方式详细讲解黑客的攻击手法和相应的网络安全管理防御技术，探究黑客Web脚本攻击核心技术，展望以后的黑客Web攻击走向和防御体系建立。
本书主要涉及黑客Web攻击中的脚本(数据库)注入技术和防御体系构建、cookies欺骗和注入攻防、新型的基于Web的DoS攻防案例，以及号称Web 2.0最大威胁的跨站脚本攻击(XSS)解析。
本书适合对网络安全技术有兴趣并想从事相关行业的大学生；就读于网络信息安全相关专业的研究生；负责企业、公司网络信息安全的从业者；网络安全技术专业研究人员；所有对网络安全有兴趣的爱好者参考阅读。

作者简介

郝永清 CISSP、CISP、MCSE资深讲师，藏锋者网络安全网(www.cangfengzhe.com)核心成员之一，主要从事信息安全相关工作，负责深入分析用户安全需求；有近十年的授课经验，为300多家企业千余IT经理及IT技术人员做过安全培训；有丰富的项目经验，同时密切跟踪国内外的安全动态，对严重安全事件进行快速响应；对各种恶意软件进行分析，提供检测和解决方案，并完成产品的安全评估，如防火墙、入侵检测、漏洞扫描等；参与众多公司网络的渗透测试项目，并对病毒和木马有深入了解。

<<黑客WEB脚本攻击与防御技术 >

书籍目录

章节摘录

插图：1.1 漫谈脚本注入脚本系统是我们最常接触的一种Web应用服务系统。
技术的发展是一个渐变渐进的过程，当下使用B／S模式编写应用程序的技术正在逐渐推广，但是负责编写程序的程序员水平和经验却参差不齐。
绝大多数程序员在编写代码的时候，由于工作量巨大、代码习惯落后、安全意识低下等原因，只顾及脚本系统功能的实现，没有进行安全性方面的考量，这就造成现在的各种脚本系统存在大量的安全隐患，也造成了基于脚本注入方面的攻击越来越多，已经成为时下网络安全中的主流热点攻击方式。
从脚本系统的构成来说，典型的脚本系统是由脚本编码加上数据库构成，其中脚本代码按编写和规范可分为ASP、PHP、JSP、ASPX等，而数据库系统常见的有Microsoft Access、Microsoft SQL Server、MySQL、Oracle等，两者分别在脚本系统中承担不同的功能和责任：脚本负责前台表现，也就是为访问者提供一个靓丽、厚重或简便的使用平台，数据库系统在后台提供数据存储，以方便各种数据的增加、修改、删除等操作。
一般情况下，数据库是隐藏在内部的，普通访问者无法直接访问数据库或者越权访问数据库中的内容。
因为脚本注入是由脚本层面发起的攻击，是以代码的方式存在。
对常规的专职网络安全管理员来讲，基本都没有深厚的脚本开发和脚本代码分析能力，自然也就对这样的攻击方式无从下手，更无法做到提前检测、修补、防护脚本漏洞。
从高于程序员编写程序的层面来说，在一般的网络安全管理员眼中，因为脚本注入（也被称为数据库注入、SQL注入等）是从正常的WWW端口访问，就和普通用户打开网站一样平凡，而且脚本注入表面看起来跟一般的Web页面访问一点区别都没有，所以一般的网络安全管理员无法及时发现这样的攻击，更谈不上修补、堵截这样的漏洞。
当前因特网上的实际情况是，因为脚本攻击的隐蔽性，很多网站、服务器被恶意黑客入侵后，在长达几个月、甚至几年的时间里，根本不会被发现。
试想，一个商业站点在长期被黑客控制的情况下何谈隐私？
何谈安全？
据权威机构统计，当下因特网中正常开放的网站，使用ASP+Microsoft Access或ASP+Microsoft SQL Server构架的占700%以上，使用PHP+MySQL构架的占20%左右，其他的构架方式不足10%。
从这个实际情况出发，本章的内容主要涉及前两种典型情况的功防技术案例，适当提及其他构架方式的相关案例。

编辑推荐

《黑客Web脚本攻击与防御技术核心剖析》主要涉及黑客Web攻击中的脚本(数据库)注入技术和防御体系构建、cookies欺骗和注入攻防、新型的基于Web的DoS攻防案例，以及号称Web 2.0最大威胁的跨站脚本攻击(XSS)解析。

四大体系深度讲解Web攻防，逾30个热点攻防案例剖析，模拟真实全面突出易读性，按图索骥实现最佳可操作性，在线平台解决新手入门。

版权说明