科爱传播
KEAI COMMUNICATIONS

郝永清［藏锋者］ 编著

网络安全攻防实用技术深度案例分析

黑客

Web脚本攻击与防御技术核心剖析

- 四大体系深度详解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难题

科学出版社
www.sciencep.com

网络安全攻防实用技术深度案例分析

黑客 Web 脚本攻击与防御技术核心剖析

郝永清［藏锋者］ 编著

科学出版社

北京

内 容 简 介

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。

图书在版编目（CIP）数据

黑客 Web 脚本攻击与防御技术核心剖析 / 郝永清编著. —北京：科学出版社，2010

（网络安全攻防实用技术深度案例分析）

ISBN 978-7-03-026011-6

Ⅰ.黑… Ⅱ.郝… Ⅲ.计算机网络–安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2009）第 205941 号

责任编辑：田慎鹏 霍志国 / 责任校对：陈丽珠

责任印制：钱玉芬 / 封面设计：耕者设计工作室

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

骏走印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2010 年 1 月第 一 版 开本：787×1092 1/16

2010 年 1 月第一次印刷 印张：23 3/4

印数：1—4 000 字数：563 000

定价：49.80 元

（如有印装质量问题，我社负责调换〈环伟〉）

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。

丛 书 序

攻防技术辩证一体

辩证的看，网络安全技术包含两个方面，正面是防御，反面是攻击，二者缺一不可：没有了攻击技术，防御技术无从谈起；没有了防御技术，攻击技术就成为摆设，没有丝毫存在的意义。

本系列书从始至终贯彻这一基本要点，和其他同类图书的最大区别就在于此。

我们虽然会详细模拟攻击者的攻击过程，但其目的是为了在防御的时候更加清楚地明白需要防御的“缺口”在什么地方。

我们也会详细讲解防御体系的搭建思路和过程，但是也会讨论突破这样的防御体系的新的攻击技术和思路，进而推出适当的防御技术。

更多的时候，本系列书的角度是在攻击者和防御者两者之间进行切换模拟——如同现在工作在岗位上的网络安全技术工程师一样，经常需要扮演攻击测试者和防护者的双重身份。

贯彻始终的“黑客”思维正面导向

有圈内人曾用“妖魔化”来形容今天的黑客，很贴切但本质很荒谬、很无奈。

原本作为褒义的“黑客”一词，是指热心于计算机技术、水平高超的电脑专家。在负面新闻不明真相的炒作下，在无数恶意攻击事件的曝光之后，在利欲熏心者的盲目追崇中，目前几乎已经完全沦为贬义的破坏者的代名词。

网络需要发展，技术需要进步。让这样歪曲的思维误导的长期后果，就是越来越多的人远离“黑客”，远离本来可能为网络发展、技术进步而提供非常大助力的群体，让原本正面积极的群体变得愈加孤僻，越加“妖魔”，甚至沦陷。

所以，本系列书坚持正面积极的正确“黑客”思维导向，并将贯彻始终，力争明晰恶意攻击者和善意黑客之间的区别，力争将攻击技术这把锋利的刀用在推动技术进步之上，力争让更多即将误入歧途的被误导者看到光明的希望！

专注于热点技术的追踪和普及

时代在变，技术也在变，技术热点的推陈出新本质就是技术进步的演变过程。关注并专注于最新的攻防技术，并将这些新的、热的网络安全技术普及给大众，

这就是本系列书的重要目标之一。

就当下的网络安全状况来看，针对 Web 服务的攻防、针对服务器的渗透攻防、针对个人计算机长期精准地控制和安全、针对网络协议的缺陷研究和修补等，都是攻击者、防御者们津津乐道的话题——自然也就是本系列书关注的话题。

需要提出注意的是，本系列书是动态的、持续变化的、跟随热点变化而进步的，所以将长期的、持续的、及时的推出！

案例化和可操作性的实现尝试

就本质来说，计算机技术是一门需要动手能力比较强的学科。作为书籍来说，可操作性的优劣将决定此书的成败。

我们采用案例化的方式来进行技术讨论，针对网络安全技术的攻击和防御两方面，采用有针对性的、螺旋上升的“攻防”对案例进行演示，力求让各技术体系毫发毕现地出现在读者面前——注意这不是空泛的理论交锋，这是可以做到“按图索骥”的一步步攻击和防御操作的详细记录！

最大化的提升书籍的易用性

任何事情的起步都是艰辛的，作为过来人的编者深刻明白迈出第一步的艰辛，所以对于刚刚接触网络安全相关领域的新手，对于理解书中相关概念略显吃力的读者，我们尽量将一些关键的概念以“基本概念解释”的方式贯穿在文中，并在书末提供速查表。目的只是为了提高系列书籍的易读性，让读者更能贴切地理解各种案例和操作中的原理。

本系列书中，类似于“基本概念解释”的还有适当位置的“技巧”、“提示”，以及序言之后的“本书使用方法”，还有文末的基本概念速查、书中所用演示平台和工具的汇总介绍等。

希望读者能将这些小项目利用起来，让其为深刻理解书中技术而起到应有的辅助作用。

辅助在线技术交流平台

做为人力有限的编者来说，遗漏在所难免，所以为了更好地为读者服务，也为了除书籍之外读者还有更方面的解惑、交流、讨论平台，本书和藏锋者网络安全网（www.cangfengzhe.com）合作，由此提供在线技术交流平台，以便本系列书的读者更快、更好、更方便地提升技术层次——当然，这个平台肯定是免费的。

部分资料来源于藏锋者

任何技术都存在表现形式上的共性，网络安全技术也不例外。正是因为存在这样的共性，在案例的选取上，本系列书使用了部分藏锋者网络上的相关资料。

这样做的原因一来是很多经典资料的确很能明白地说明问题；二来是因为很多典型技术的推出就是因为存在这样的典型案例；三则是出于对实用性的考虑——我们倡导的方式是读者在通读全书后，去藏锋者网站下载并搭建书中案例的相关环境，使用相关工具进行模拟攻击和模拟防护，已达到真正将书中的技术纳为己有的目的。

纠错及感谢

编著过程仓促，难免有所遗漏或者错误，如有发现，欢迎读者使用上述的网络交流平台与编者联系，提前致谢。

在系列书编著过程中，得到很多藏锋者网络上的技术伙伴们的支持和帮助，在此一并感谢。

最重要的是，系列书的出版和推出，得到科学出版社的大力支持。特别是责任编辑田 sir，事前、事中、事后均提供了莫大的支持，鞠躬谢过。

郝永清

2009 年 9 月于北京

代　序

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。另外作者提出的针对 Web 服务的 DDoS 攻击也很有前瞻性，至于号称 Web 2.0 时代的最大威胁：跨站脚本攻击（XSS），目前还鲜有系统全面而紧跟实例的文字资料，作者在本书中也做了详细阐述并使用了一些典型案例进行

模拟……上述的内容中，不管是普及也好，还是前瞻讨论也好，都是紧扣现实的网络安全技术，也就是最具有正面意义的社会责任感的积极体现，就能让更多被误导而妖魔化攻防技术的人真正看清究竟什么是遭人唾弃的攻击者，什么是真正研究技术的“黑客”。

一本网络安全技术的普及类书籍，无非在两种特色之间取舍：全面细致的原理分析亦或案例模拟。本书作者用了一种两者相结合的方式来进行编著，案例模拟部分采用了比较新颖的“按图索骥”的方式来叙述，读者的可操作性还是比较高的；另一方面，本书的原理分析略显单薄，但是作者比较巧妙地在书中安插了一些科普类的“基本概念解释”，有助于特别是新手对整个网络安全体系进行系统了解，对技术体系的普及也有一定意义。

多说无益，最终决定此书好坏的人还是读者自己，就好比最终决定网络安全技术走向的依然是网络安全参与者一样。

同为卑微的参与者，愿为网络安全正名！

独行者

2009 年 10 月于北京

本书使用方法

请用虚拟机

对任何一个网络安全技术爱好者来说，虚拟机都是必须的，也是必要的。

如果读者对本书中所讲案例有兴趣，想亲手操作，以达到最佳的阅读和理解效果，请使用虚拟机在本地虚拟相关系统，并在虚拟机上使用相关工具进行攻击和防御测试。

使用虚拟机的最大目的在于保障读者自身的系统安全；

其次是为了杜绝不经意间由读者兴趣而引发的网络恶意攻击；

然后是为了读者更深刻地理解不同身份的攻击者和防御者的操作平台、操作方法和操作目的；

最后是为了读者养成网络安全技术的基本构建、调试习惯，为以后可能遇到的网络安全问题提供最基本的环境支持。

基本概念解释

文中适当位置将出现“基本概念解释”，一般情况下是对上文中和本书主题无关，但却因为案例需要而有所涉及的理论概念。

整个网络安全体系庞大到难以想像，对于有一定经验的读者来说，将文中所述技术和其他相关概念联系在一起是很有裨益的，对技术层次的提升和某方面技术的全面透彻的理解尤为重要。

对于刚刚接触网络安全技术的读者来说，直接的案例风格书虽然可以很方便地提高读者的操作兴趣，快速让读者获得某一领域的相关技术理解，但是未免太过于片面、单调。所以，对于新手来说，“基本概念解释”将是一个比较有用的全面的理解网络安全体系的机会，有关联的相关概念更能让新手在脑中构建完整的网络安全体系图。

当然，如果是已经有深入研究的读者，阅读此书只是因为想了解其中最新的技术，大可略过这些内容。

提示

书中适当位置将有“提示”出现，“提示”的作用是编者对特定环境和情况的

说明。

例如是为了演示这个案例而进行的非常规操作，在实际情况中不建议使用这样的操作。

简单来说，“提示”就是编者因为行文需要，为了避免误导读者而做的防护措施。

技巧

和“基本概念解释”、“提示”不同，需要特别指出的是，“技巧”一般是以攻击者的角度给出的说明，这些说明一般是针对特定环境的非常有效的攻击手法。

书中可能出现为了全盘需要，模拟攻击者进行攻击的时候，没有使用最好的、最灵巧的、最直接的攻击方式，而是采用了和书中相关概念深度符合的基本手法进行攻击模拟，故以“技巧”的方式补充说明。

案例相关工具和程序平台

网络安全技术很多时候在明白原理之后，不用自己编写相关工具，网络上已经有很多前人编写了适当的攻击和防御工具，所以“站在巨人的肩上”是最好的快速进步的方法。

书中的相关工具除了在对应的章节出现以外，还在文末有统一的附件形式速查。

另外藏锋者网络也专门为本书提供了相关工具和程序平台的下载支持，读者可以浏览并下载。

编者建议读者在虚拟机中搭建这样的相关环境，然后同样在虚拟机中使用相关工具进行攻击模拟和防御模拟。

在线交流

为了给各技术层次的读者提供及时在线的交流平台，本书和藏锋者合作提供了一个免费的在线交流平台。

读者可以通过登录藏锋者网站（www.cangfengzhe.com）进行技术交流。

编者邮件

编著过程比较仓促，难免出错，欢迎发现错误的读者与编者联系：cangfengzhe@live.cn。

目　录

第 1 章　脚本（数据库）注入与防注入核心技术

章节内容提点与概述

本章主要内容：

- ■ 注入核心原理与隐蔽性、危害性
- ■ 典型流程与规范代码剖析
- ■ 注入攻击典型案例模拟
- ■ 防注入 17 条核心法则
- ■ 深度注入防范技术案例

本章典型案例：

- □ ASP 注入案例
- □ PHP 注入案例
- □ JSP+Oracle 注入案例
- □ ASP 防注入函数编写
- □ PHP 防注入函数编写

本章核心概念：

● 脚本注入，也叫数据库注入、SQL 注入（SQL injection），是通过把 SQL 命令插入 Web 表单递交或输入域名、页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令的一种攻击方式。

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 70%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。

本章将先和读者一起，理清脚本注入攻击的核心理念，然后模拟分析各种典型黑客攻击案例，进而总结、推导出有针对性的防范技术，最后再以实际的防范

代码、案例为结尾。希望通过可操作性非常强的各个案例讲解，让读者不但清楚知道如何防范这样的攻击，更能完全明白基于脚本系统的各种攻击是如何发起进行的，以达到技术上“知其然且知其所以然”的讨论研究目的。

1.1.1　注入核心原理

任何事物产生都有其根源，掌握根源才能充分掌握它们的性状、态势，才能彻底了解相关习性和常规方式。

注入攻击也是这样，深入了解注入的构成和核心原理，对攻击者来说可以达到事半功倍的目的，对防御者来说在需要构建防御体系的时候，从根源上堵住缺陷才是最根本的做法。

1.1.1.1　什么是脚本注入

在 Web 脚本攻击中，脚本注入是最普遍、最容易发起、最容易搞破坏、最容易出纰漏的地方，那首先解决一个问题：究竟什么是脚本注入？

所谓脚本注入，也叫数据库注入、SQL 注入（SQL injection），就是通过把 SQL 命令、SQL 语句插入 Web 表单递交或输入域名、页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令的一种攻击方式。

> **基本概念解释**：什么是 SQL?
>
> SQL 全称是“结构化查询语言”（structured query language），是一种数据库查询和程序设计语言，用于存取数据以及查询、更新和管理关系数据库系统。它允许高级的非过程化编程语言，允许用户在高层数据结构上工作。

1.1.1.2　脚本注入产生的根源

对于一个 Web 应用平台来讲，不管是论坛、网页还是其他功能，都是由脚本加上数据库而存在的，当今绝大多数 Web 应用平台，都是通过 B/S 模式来实现，使用 B/S 模式来编写程序的程序员也越来越多，但是由于程序员的水平参差不齐，相当一部分应用程序存在安全隐患。

> **基本概念解释**：什么是 B/S 模式?
>
> B/S（browser/server，浏览器/服务器）模式又称 B/S 结构。它是随着 Internet 技术的兴起，对 C/S 模式应用的扩展。在这种结构下，用户工作界面是通过 IE 浏览器来实现。B/S 模式最大的优势是运行维护比较简便，能实现不同的人员从不同的地点，以不同的接入方式（如 LAN、WAN、Internet/Intranet 等）访问和操作共同的数据。