网络安全专家

网站入侵与脚本攻防修炼

- Web入侵揭秘

SQL注入流行一时 | 上传漏洞危害严重 | 暴库泄露机密 | Cookie欺骗阴险狡诈 | 跨站借刀杀人……

- 权威分析，深入漏洞成因
- 全真范例，再现攻击实景
- 光盘包含数十个黑客攻击演示动画与配音视频

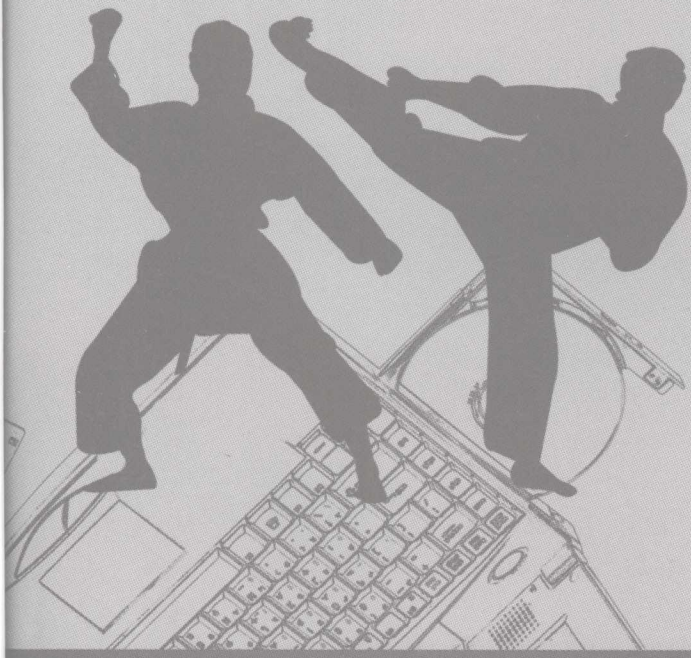
肖 遥 编著
飞思科技产品研发中心 监制

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

CD-ROM
随书光盘包含视频教程、演示动画与章节源代码

网络安全专家

网站入侵与脚本攻防修炼



肖　遥　编著
飞思科技产品研发中心　监制

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

内容简介

本书从“攻”、“防”两个角度，通过现实中的入侵实例，并结合原理性的分析，图文并茂地展现网站入侵与防御的全过程。全书共分 8 章，系统地介绍网站入侵的全部过程，以及相应的防御措施和方法。其中包括网站入侵的常见手法、流行网站脚本入侵手法揭密与防范、远程攻击入侵网站与防范、网站源代码安全分析与测试等。本书尤其对网站脚本漏洞原理进行细致的分析，帮助网站管理员、安全人员、程序编写者分析、了解和测试网站程序的安全性漏洞。本书用图解的方式对网站入侵步骤及安全防范设置都进行详细的分析，并且对一些需要特别注意的安全事项进行重点提示，过程中还加入一些安全技巧。

随书所配光盘内容包括书中涉及的源代码、视频教程和演示动画，方便读者学习和参考。

本书适合于网络安全技术爱好者、网络管理员、网站程序编写人员阅读，也可作为相关专业学生的学习及参考资料。

图书在版编目（CIP）数据

网站入侵与脚本攻防修炼 / 肖遥编著.—北京：电子工业出版社，2008.9
（网络安全专家）
ISBN 978-7-121-07005-1

Ⅰ. 网… Ⅱ. 肖… 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（2008）第 095540 号

责任编辑：王树伟　田　蕾
印　　刷：北京机工印刷厂
装　　订：三河市鹏成印业有限公司
出版发行：电子工业出版社
　　北京海淀区万寿路 173 信箱　邮编：100036
开　　本：720×1 000　1/16　印张：36.25　字数：812 千字
印　　次：2008 年 9 月第 1 次印刷
印　　数：5 000 册　　定价：59.00 元（含光盘 1 张）

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。

前　言

据统计，大约每 20 秒就有一次网络入侵事件的发生，全球每年因网络安全问题造成的经济损失高达数百亿美元。在我国，90%以上的网站存在安全漏洞，很多网站都曾受到过黑客的攻击和计算机病毒的侵害。

为何网站如此难以确保安全？为何一个学习了几个小时的“脚本小子”，竟能轻易地入侵并控制你的网站？为何拥有众多安全专家的大型网站，却也防不住一个狡猾黑客的攻击？——这一切都缘于 Web 网页脚本攻击！

如今，市面上各种安全书籍种类繁多，而专门针对各种网站脚本攻击进行深入分析的书籍是鲜有见者。而伴随网络的普及与发展，各种网站攻击事件频频出现，提高网站安全意识与掌握安全防范技术迫在眉睫。许多网页设计者与网站管理员，安全技术研究人员，甚至个人安全爱好者，都急需了解 Web 网页脚本攻击技术，以便更好地设计程序、管理网站及进行攻击事件分析。

于是，本书便应各类读者所需编写出版，对各种网站脚本攻击技术进行深入的介绍与分析，并给以详细的攻击重现演示，相信一定能让读者对网站脚本攻击技术有一个全面、深入的了解。

尤其值得一提的是，本着“授人以渔”的原则，本书对各种典型的网站脚本漏洞进行详细的代码分析，试图让读者通过典型的漏洞分析，了解此类攻击脚本漏洞出现的原因，以及相关的防范方法，以便达到举一反三的目的，从而学会自己检测分析网站程序漏洞。相信对网站程序设计者、网站管理员和安全技术研究人员都是有益的，各类读者一定能从中汲取到有价值、有意义的东西。

由于编者水平有限，时间紧促，书中难免有不足之处，敬请读者批评指正。

编　著　者

联系方式

咨询电话：（010）68134545　88254160

电子邮件：support@fecit.com.cn

服务网址：http://www.fecit.com.cn　http://www.fecit.net

通用网址：计算机图书、飞思、飞思教育、飞思科技、FECIT

光盘目录

[视频教程]

Google 暴库漏洞.rmvb

Google 是一个强大的搜索引擎，没有想到 Google 也可以搜索出网站程序的数据库漏洞吧？利用 Google 爆出网站的数据库下载入侵网站。

替换空格的注入攻击.rmvb

在各种网站源程序中，对空格进行过滤是很常见的一种 SQL 注入防护手段，本视频演示如何用字符替换空格进行注入攻击。

漏洞站点的挖掘鸡（上）.rmvb

漏洞站点的挖掘鸡（下）.rmvb

“挖掘鸡”是一款强大的网站漏洞挖掘检测工具，本视频演示利用该工具批量搜索检测网站漏洞进行攻击。

通过数据库备份后台拿 webshell.rmvb

数据库备份拿 Webshell 是一种很常见的后台上传 Webshell 木马后门方法，在动网老版本及很多网站程序后台都可以利用此方法控制网站服务器。

[演示动画]

9Cool 九酷空间管理系统上传漏洞演示

9Cool 九酷空间管理系统是一个非常流行的建站服务空间管理系统，此系统存在一个文件名绕过上传漏洞，本动画演示通过修改上传文件名的后缀绕过程序检测，实现上传 ASP 及 ASA 等木马后门的过程。

Access 注入点猜解表名及字段名的数据长度

在 SQL 注入中，通过 Access 注入点猜解数据库表名及字段名是比较麻烦的事情，本动画完整演示对某网站注入点的猜解，便于大家直观了解猜解过程中需要注意的相关事项。

Access 注入猜解表名及字段名的实例

本动画接上面的动画，构成完整的 Access 注入猜解过程，通过已知的表和字段，猜解出 Access 数据库中的任意数据。

ASP 木马后门的免杀及隐藏

ASP 木马后门的免杀及隐藏 2

在 Web 入侵中，上传木马后门 Webshell 控制网站服务器是不可缺少的步骤，但是上传的木马后门常常被杀毒软件或管理员手工查杀掉。本动画讲解 ASP 木马后门免杀躲过杀毒软件，并讲解如何隐藏 ASP 木马后门，让管理员难以发现，其他类型的木马后门也可以用同样的方法进行查杀。

BBSXP 暴库漏洞

本动画演示了典型的 BBSXP 暴库漏洞利用，包括爆出数据库地址，下载数据库，破解管理员密码及后台登陆控制网站。

使用工具进行 SQL 注入攻击

自动化进行 SQL 注入攻击的工具非常多，本动画演示使用 NBSI 工具进行 SQL 注入攻击，实现数据库表名字段及数据的自动化猜解，以及后台管理员登陆页面的扫描。

入侵 NB 文章系统 1

入侵 NB 文章系统 2

NB 文章系统中存在着 FCKeditor 插件漏洞，该漏洞是一个典型的文件上传漏洞，本动画演示通过修改上传链接实现突破限制上传 ASP 后门的目的。

天意商务网上传漏洞演示（补充）

天意商务网上传漏洞演示

网上有许多上传漏洞利用工具，但本动画示例的是手工进行上传攻击。利用天意商务网的上传漏洞，通过 WSockert 嗅探工具抓包，然后修改上传数据，使用 NC 工具进行提交攻击。

将 ASP 木马后门与图片合二为一

ASP 木马如何更隐蔽地躲过查杀？本动画提供将 ASP 木马后门藏在图片中的方法，既不影响 ASP 后门的使用，又极难被管理员发现！

阿 D 工具快速控制网站

阿 D 注入工具是一个常用的 SQL 注入工具，本动画演示的是利用注入点的 SA 权限，快速获取网站控制权，看了动画，你会觉得入侵一个网站是如此地简单！

[章节源代码]

\Ch2\1.2.3 SQL 注入简单实例.rar（一个 SQL 注入点模拟的程序代码）

\Ch2\1.6.3 SQL 高级查询之 Group By 和 Having.mdb

\Ch2\1.6.4 联合查询.mdb

\Ch2\1.6.5 连接查询.mdb

\Ch2\MySQL 控制程序示例.rar

\Ch2\MySQL 查询浏览工具 .rar

\Ch2\test.mdb

\Ch2\典型的密码验证漏洞代码——织梦.rar（织梦系统是一个存在密码验证漏洞的典型网页程序，可利用 or '1'='1 经典漏洞绕过登陆验证）

\Ch2\用 ASP 直接存取 ACCESS 数据库实例.rar

\Ch3\BBSXP 源代码.rar

\Ch3\SQL 通用防注入代码.rar（可防范 SQL 注入攻击的代码，在各网页中使用 include 调用包含即可）

\Ch3\使用 Access 数据库的 dvbbs 源代码.rar

\Ch3\使用 SQL 数据库的 Dvbbs 源代码.rar

\Ch3\使用 SQL 数据库的 oblog 代码.rar

\Ch3\转换单引号注入示例——SQLInjectEncode.rar（使用 SQLInjectEncode 可轻松地突破网页程序对单引号的过滤）

\Ch4\conn.asp

\Ch4\test.asp

\Ch4\testxiaoyao2008.mdb

\Ch4\存在暴库漏洞的 BBSXP 源代码.rar（BBSXP 中存在典型的暴库漏洞，可供分析）

\Ch5\Joekoe 乔客上传漏洞源代码.rar（Joekoe 乔客上传漏洞源代码中可分析文件名过滤不严的上传漏洞原因）

\Ch5\Mtthew1471 BlogX 上传漏洞源代码.rar

\Ch5\NEATPIC 上传漏洞源代码 v1.2.3.rar（典型的 PHP 文件上传漏洞成因源代码分析）

\Ch5\phpcms 上传漏洞源代码.rar

\Ch5\SLBlog 上传漏洞源代码.rar

\Ch5\九酷空间管理系统上传漏洞源代码.rar（文件名过滤不严的典型漏洞代码）

\Ch5\动力 MyPower 上传漏洞源代码.rar

\Ch5\动感下载系统 XP 上传漏洞源代码.rar

\Ch5\动感购物上传漏洞源代码.rar

\Ch5\十三 WebShell 9.0 示例.rar（一个功能非常强大的 ASP 木马后门代码，可实现网站目录浏览、文件上传下载、在线文件管理，提权与执行命令等功能）

\Ch5\天意商务网上传漏洞源代码.rar

\Ch5\桃源多功能留言板上传漏洞源代码.rar

\Ch5\沁竹音乐网上传漏洞源代码.rar（这是一个由于程序权限限制不严格，任意用户可调用危险网页程序生成 Webshell 后门的典型漏洞代码）

\Ch5\沸腾 3AS 流浪尘缘新闻系统上传漏洞源代码.rar

\Ch5\网站上传利用程序示例.rar

\Ch5\网站安全综合检测示例.rar

\Ch5\自由动力上传漏洞源代码.rar

\Ch5\飞龙文章管理系统上传漏洞源代码.rar

\Ch6\JIMMY 留言簿 Cookie 欺骗漏洞源代码 .rar

\Ch6\L-BlogCookie 欺骗漏洞源代码.rar（L-Blog 中的欺骗漏洞，可通过依靠 Cookie 信息中的用户等级字符，实现伪造管理员身份，该漏洞成因的代码显示）

\Ch6\商贸通 Cookie 欺骗漏洞源代码.rar

\Ch6\艸坤论坛 Cookie 欺骗漏洞源代码.rar

\Ch7\业一新闻系统跨站代码.rar（业一新闻系统存在跨站漏洞过滤不严的代码）

\Ch7\时代购物系统跨站漏洞代码.rar

\Ch8\SQL 通用防注入代码.rar（可实现防整站的 SQL 注入攻击的源代码，可修改后实现更强大的过滤功能）

目　录

第1章 网站脚本入侵与防范概述

在网络异常发达的今天，网络上各种大大小小的网站已经随处可见。博客、文章系统、论坛、相册、留言本、投票系统等，各种各样的站点为网络平添许多色彩。无论是从公司、企业，还是个人，往往都会拥有自己的网站，网站已经成为交流沟通、展示个性、商业宣传等必不可少的手段。

然而，在网络丰富而精彩的世界中，也正潜藏着一道道危险的暗流。各种各样的网站攻击事件层出不穷，大到国家政府部门，小到单位、个人的站点，都常常出现被入侵攻击事件的报道。

为何网站如此难以确保安全？为何一个学习了几个小时的“脚本小子”，竟能轻易地入侵控制你的网站？为何拥有众多安全专家的大型网站，却也防不住一个狡猾黑客的攻击？——这一切，源于网站脚本的脆弱性，也有众多网站程序设计者与管理员对网站入侵技术的陌生有着重要的关系。

Web 应用程序的代码，并不像意想中的那样安全；但维护 Web 网站程序的安全性，也并非无章可寻。本书要带给大家的，将是揭示各种网站脚本入侵技术行为，并详细分析其原理与相关的防护方案，为网站程序设计者及管理人员找到一条安全之道。

1.1 危害严重，难于防范的 Web 脚本入侵攻击

尽管网络在不断的发展，网站服务器安全意识与知识的普及状况也比几年前

好了很多，但是各种网络脚本入侵攻击事件反而愈演愈烈。

据统计，大约每 20 秒就有一次网络入侵事件发生，全球每年因网络安全问题造成的经济损失高达数百亿美元。在我国，90%以上的网站存在安全漏洞，很多网站都曾受到过黑客的攻击和计算机病毒的侵害。

虽然许多网站做了大量的安全工作，安装防火墙保护服务器，给系统打上最新的补丁，安装各种攻击检测系统，但依然不能阻挡黑客的入侵攻击。而这一切攻击来源最猛烈之处，就是网站上的各种 Web 应用程序。

各种 Web 应用程序，让网站陷入异常尴尬的局面——网站在不得不提供相应服务的同时，却又无法保证程序的安全性。这是一个两难的问题。

的确如此，各种针对 Web 应用程序的脚本攻击技术，将各种大大小小的网站服务器都置于极为危险的境地。这种攻击方式破坏性极强，轻者让网站无法正常服务和访问，重者直接导致服务器数据丢失，被黑客控制！

1.1.1 Web 脚本攻击概述及特点

Web 站点默认 80 为服务端口，关于它的各种安全问题不断地发布出来，这些漏洞中一些甚至允许攻击者获得系统管理员的权限进入站点内部。许多黑客甚至可以突破 SSL 加密和各种防火墙，攻入 Web 网站的内部，进而窃取信息。黑客可以仅凭借浏览器和几个技巧，就能获取 Web 网站的客户保密资料，甚至控制整个网站服务器。

简单来说，针对网站服务器 80 端口的 Web 服务进行的各种攻击行为，就叫做 Web 脚本攻击。

Web 脚本攻击入侵，在网络上非常泛滥，原因也在于其特殊性，见如下说明。

1. 暴露的目标

由于网络上各种大大小小的网站数不胜数，因此给 Web 脚本攻击者提供了众多的攻击目标。同时 Web 脚本攻击的目标不仅在于公司和政府等大型网站，同时也威胁着各种个人网站；而 Web 脚本攻击不仅应用在常见的 Windows 操作系统上，对于 UNIX、Tomcat 等众多类型操作系统的服务器上，Web 脚本攻击也能顺利地展开实施。同时无论是任何 Web 服务程序，都有存在可攻击漏洞的可能。

可以这么说，只要用网站的地方，就存在着 Web 脚本攻击。正是由于 Web 脚本攻击的目标极为众多，也导致了 Web 脚本攻击事件的频繁发生。

2. 危害严重

普通的木马攻击和程序溢出漏洞攻击等，都可以获得攻击目标主机操作系统

的控制权利，而 Web 脚本攻击的危害同样严重。

使用 Web 脚本攻击，不仅可以轻易地更改目标主页信息，导致网站服务无法正常进行，重者可以盗取网站用户中的重要数据，造成整个网站瘫痪，甚至还可以控制整个网站服务器。

同时，由于网站服务器一般都属于目标网络系统中比较重要的主机，因此在渗透入侵攻击整个目标网络时，Web 脚本攻击都将起到极具破坏力的作用。

Web 脚本攻击的危害严重，还体现在 Web 脚本攻击的简单性上。由于 Web 脚本攻击采取的手段往往很简单，也许一句话的代码就可以让网站服务器被黑客控制掌握于掌指之中。而许多网站管理员门往往只是对系统的安全特性比较重视，却忽略了网站 Web 程序方面的漏洞，由于防范的疏忽，因此使用的 Web 脚本攻击比一般的攻击方式更易进行，对网站服务器造成的危害更大。

3．攻击方式多样

由于 Web 网站服务器各异，使用的网站程序也不尽相同，不同的 Web 网站服务器和不同的网站程序都可能存在不同的漏洞，因此使用 Web 脚本攻击方式极为多样。

Web 脚本攻击者可能从网站的文章系统、下载系统、留言板等部分进行攻击，也可能针对网站的数据库进行操作，也可能在网页中写入攻击性的代码等。甚至于通过网站上的一幅图片，都可以进行攻击，因此 Web 脚本攻击可谓无孔不入。

4．难于防范

对于普通的攻击方式，如木马攻击、溢出攻击等，网络管理员可以通过为操作系统打上各种安全漏洞补丁、安装防火墙和杀毒软件等进行防范，而这些防范措施也往往是有效的。但是对于 Web 脚本攻击来说，这些防范方式往往很难有较好的效果。

由于每个网站采用的 Web 程序都不相同，因此每个网站可能存在的漏洞也不相同，很难采用统一的方式为网站进行补漏、打补丁。

与一般的入侵攻击方式相比，Web 脚本攻击不会在防火墙和系统日志中留下任何入侵痕迹，即使经历丰富的网络管理员，也很难从网站日志中追查出入侵者的足迹。

5．不易检测

一般的入侵攻击方式，往往会由于攻击目标上安装了防火墙而导致失败，但是使用 Web 脚本攻击的话，防火墙却形同虚设。由于 Web 脚本攻击的所有操作

都是通过系统中的 80 端口来进行的，而通过该端口的数据都是被防火墙所许可的，因此防火墙不会对 Web 脚本攻击进行拦截，使得 Web 脚本攻击可以顺利地通过防火墙进行。

同时入侵者通过 Web 脚本攻击入侵后，往往是通过在网站中放置一些 ASP 或脚本代码文件作为后门，这些文件往往很难像普通的病毒那样可以通过杀毒软件查杀。更有甚者，在合法的网页文件中插入一段隐蔽的代码，致使杀毒软件完全无法识别这样的后门存在。还有的入侵者直接修改网页源代码，取消某些密码验证等，使入侵者可以随意自由地进入服务器，对于这些留后门的方式，杀毒软件可以说是完全无效了。

1.1.2 入侵者是怎样进入的

Web 脚本攻击的一个突出特点，就是攻击手段方式多种多样，攻击者在进行 Web 脚本攻击入侵时，通常会采取哪些步骤呢？

1. 踩点

所谓“踩点”，与普通入侵方式中的系统扫描类似，就是通过各种手段来对要入侵的网站服务器进行分析和判断，从而寻找到服务器可能存在的漏洞，并决定采取何种入侵方式才能最快、最隐蔽地成功入侵网站服务器。

踩点所要获取的信息包括以下内容。

1）操作系统与服务器版本

不同的网站服务器采用的操作系统不同，主要有 Windows 系统、UNIX 系统、Linux 系统及 Tomcat 系统等。

在 Windows 操作系统中常见的网站服务程序为 IIS，版本也不尽相同，比如 Windows 2000 系统使用的是 IIS 5.0，而 Windows XP 系统使用的则是 IIS 6.0 版本。在 UNIX 系统、Linux 系统中常见的网站服务程序是 Apache，版本也不相同。而许多 JSP 网站程序服务器则使用了比较少见的 Tomcat 系统。

不同的操作系统入侵方式也不同，如在 Tomcat 3.0 版本中就存在一个目录路径泄露漏洞，而在 IIS 服务器中则有可能存在暴库、脚本备份后门等漏洞，因此攻击者在实施 Web 入侵攻击前，首先会获得网站服务器的操作系统及网页服务器版本信息，并制订出合适的入侵方案来。

2）Web 程序结构

由于每个网站使用的 Web 程序不同，有可能是公开的源代码，也有可能是网站自己撰写的程序。攻击者首先要了解到 Web 程序的各种信息，如首页