

<<网站入侵与脚本攻防修炼>>

图书基本信息

书名：<<网站入侵与脚本攻防修炼>>

13位ISBN编号：9787121070051

10位ISBN编号：7121070057

出版时间：2008-9

出版时间：逍遥 电子工业出版社 (2008-09出版)

作者：逍遥

页数：566

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<网站入侵与脚本攻防修炼>>

### 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。

## <<网站入侵与脚本攻防修炼>>

### 内容概要

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。

## <<网站入侵与脚本攻防修炼>>

### 作者简介

肖遥，男，1979年生。

笔名“冰河洗剑”，职业IT撰稿人，著名电脑安全技术研究者。

2001年毕业于贵州工业大学，曾任职贵州安顺风雷军械厂助理工程师，参与过J10A、J11B等战斗机配套武器研制，独立开发出HF25火箭发射器，参与DF8GA及导弹发射架等武器设计。

现居贵州省六盘水市，长期为安全类杂志《黑客x档案》、《黑客防线》等杂志撰写安全类稿件，也是国内知名电脑杂志《电脑迷》、《大众软件》、《网友世界》、《电脑报》特约作者。

撰稿6年，累计发表报刊作品达赢百余万字，出版《黑客大曝光》、《黑客成长日记》、《无毒一身轻》、《病毒与黑客攻击技术》等十余部电脑网络安全畅销书籍。

## &lt;&lt;网站入侵与脚本攻防修炼&gt;&gt;

## 书籍目录

第1章 网站脚本入侵与防范概述. 11.1 危害严重, 难于防范的Web脚本入侵攻击 11.1.1 Web脚本攻击概述及特点 21.1.2 入侵者是怎样进入的 41.2 脚本漏洞的根源 61.2.1 功能与安全难以兼顾 71.2.2 安全意识的缺乏 7第2章 SQL注入, 刺入网站的核心 92.1 SQL注入的目标是数据库 92.1.1 数据库就是网站的一切内容 102.1.2 明白几个SQL中要用到的名词 112.1.3 SQL注入攻击中常碰到的几种DBMS 122.1.4 提前了解几条SQL注入查询指令 142.2 欺骗是如何进行的 162.2.1 一个无名小站与一条典型SQL语句 162.2.2 创建SQL注入检测的数据库平台 192.2.3 搭建一个SQL注入漏洞站点 262.2.4 第一次SQL注入攻击测试 292.3 SQL注入攻击前奏 312.3.1 网站平台决定攻击方式 312.3.2 攻击前的准备工作 322.3.3 寻找攻击入口 362.3.4 区分SQL注入点的类型 422.3.5 判断目标数据库类型 432.4 'or'='or'绕过不安全的登录框 492.4.1 'or'='or'攻击突破登录验证的演示 502.4.2 未过滤的request.form造成注入 522.5 注入Access数据库全靠猜解 592.5.1 信息很丰富的Select查询 592.5.2 使用Select猜解Access表及字段名 662.5.3 ASCII逐字解码法猜解字段值 722.5.4 三分钟攻陷了一个网站 792.5.5 网站是怎样被控制的 892.6 为MS SQL带来灾难的高级查询 932.6.1 建立MS SQL数据库进行攻击演示 932.6.2 有趣的MS SQL出错信息 972.6.3 SQL高级查询之Group By和Having 992.6.4 报出MS SQL表名和字段名的实例 1032.6.5 数据记录也“报”错 1062.6.6 继续前面的“入侵” 1082.6.7 报出任意表名和字段名 1102.7 扩展存储过程直接攻击服务器 1112.7.1 存储过程快速攻击数据库 1112.7.2 利用NBSI注入控制服务器 1132.8 构造PHP注入攻击 1162.8.1 手工PHP注入 1162.8.2 读取PHP配置文件 1182.8.3 CASI自动PHP注入 120第3章 深入SQL注入攻击与防范 1233.1 一厢情愿的过滤, 缺失单引号与空格的注入 1233.1.1 转换编码, 绕过程序过滤 1243.1.2 /\*\*/替换空格的注入攻击 1283.2 Update注入与差异备份 1493.2.1 表单提交与Update 1493.2.2 差异备份获得Webshell 1533.3 char字符转换与单引号突破 1603.3.1 \0与单引号的过滤 1603.3.2 char再次绕过单引号 1623.4 数据提交与隐式注入 1683.4.1 修改GroupID, 迅速提升权限 1683.4.2 隐式注入中的过滤突破 1803.5 卡住SQL注入的关口 186第4章 未隐藏的危机——数据库入侵 1894.1 “暴露”易受攻击——常见数据库漏洞 1894.2 了解一些数据库连接知识 1914.2.1 ASP与ADO对象模块 1914.2.2 ADO对象存取数据库 1934.2.3 攻击与安全的核心——Access数据库连接代码示例 1944.3 安全意识的缺乏——默认数据库下载漏洞 1954.3.1 模拟一个论坛搭建流程 1954.3.2 被入侵者钻了空子 1974.3.3 入侵者找空子的流程 1994.4 数据库被下载, 后果很严重 2024.5 黑名单, 别上榜 2134.5.1 看看你是否在榜 2134.5.2 别懒, 动手解决安全隐患 2144.6 诡异的Google, 低级的错误 2174.6.1 很诡异的搜索试验 2174.6.2 居然能下载 2194.6.3 Google的暴库分析 2214.6.4 上一个Include解决问题 2234.7 为何攻击者偏偏盯上你 2234.7.1 漏洞站点的挖掘“鸡” 2244.7.2 网站数据库, 不藏就抓 2244.7.3 Robots看门, 阻止搜索暴库数据 2274.8 隐藏数据库, 暴库即知 2314.8.1 ASP存取Access数据库的例子 2314.8.2 游戏1: 变换编码的魔术 2344.8.3 魔术的秘密 2374.8.4 游戏2: 奇怪的conn.asp 2434.8.5 绝对路径与相对路径的纠缠 2444.8.6 “on error resume next”——补上不算漏洞的漏洞 2454.9 几个暴库程序的分析.. 2474.9.1 动感商城购物系统暴库漏洞测试 2474.9.2 无法下载的ASP数据库——BBSXP的暴库测试 2524.9.3 带#号的数据库——Oblog博客系统暴库 2574.9.4 conn.asp搜索暴库 2594.10 “空白”与插马——GBook365暴库入侵的启示 2614.10.1 方便了设计者, 也便宜了攻击者的conn.inc 2614.10.2 乱改后缀的后果 2624.10.3 黑手后门就是数据库 2644.10.4 严过滤, 堵住漏洞 2704.11 由启示引发的一句话木马大攻击 2714.11.1 “一句话”与数据库过滤不严 2714.11.2 一句话木马客户端与服务端 2724.11.3 实例1: 一个私服站点的湮灭 2724.11.4 实例2: 一句话入侵EASYNEWS 2794.11.5 实例3: “社区超市”入侵动网论坛 2824.11.6 实例4: 对未知网站的检测 2844.11.7 有输入, 便有危险——一句话木马的防范 285第5章 程序员的疏忽, 过分信任上传 2875.1 多余映射与上传攻击 2875.1.1 来自asp.dll映射的攻击 2885.1.2 别忘了stm与shtm映射 2945.2 空格.点与Windows命名机制产生的漏洞 2995.2.1 加上一个点, 9Cool九酷的另一个漏洞 2995.2.2 Windows命名机制与程序漏洞 3005.2.3 变换文件名的游戏 3025.3 逻辑变量的怪圈, 二次循环产生上传漏洞 3075.3.1 攻击者“动力”——MyPower上传攻击测试 3075.3.2 本地提交上传流程分析 3125.3.3 二次上传产生的逻辑错误 3155.3.4 再现经典上传, “沁竹音乐网”漏洞分析 3175.3.5 补又有漏洞的“桃源多功能留言板” 3215.4 Windows特殊字符, 截断程序过滤 3275.4.1 脚本入侵探子WSockExpert与上传攻击 3285.4.2 截止符00与FilePath过滤漏洞 3365.4.3 00与FileName过滤漏洞 3435.5 FilePath与Filename变量欺骗大检测 3505.5.1 桂林老兵上传漏洞利用程序 3505.5.2 检测天意商务网上传漏洞 3575.5.3 检测飞

## &lt;&lt;网站入侵与脚本攻防修炼&gt;&gt;

龙文章系统上传漏洞 3595.5.4 检测BlogX上传漏洞 3625.5.5 检测动网大唐美化版上传漏洞 3645.5.6 检测尘缘新闻系统上传漏洞 3655.5.7 检测乔客Joekoe论坛上传漏洞 3675.5.8 击溃青创文章管理系统 3685.6 %00与PHP程序的上传漏洞 3695.6.1 NEATPIC相册系统 3695.6.2 文件类型过滤不严, phpcms文件上传漏洞 3725.7 暗藏漏洞的第三方插件 3755.7.1 导致网站崩溃的FCKeditor 3765.7.2 无处不在的FCKeditor上传漏洞 3785.7.3 eWebEditor密码与上传漏洞的结合 3825.8 意料之外的上传 3865.8.1 未加权限的上传——沁竹音乐程序上传漏洞 3865.8.2 ccerer——不受控制的字符过滤游戏 3895.8.3 上传漏洞藏不住 394第6章 入门牌的泄露与欺骗——Cookie攻击 3976.1 混乱的代码与欺骗的实例 3976.1.1 Cookie信息中的安全隐患 3996.1.2 进入后台竟然如此简单 3996.1.3 不是管理员竟然可删帖 4056.2 深入Cookie信息的修改欺骗 4136.2.1 数据库与Cookie信息的关系 4146.2.2 Cookie欺骗与上传攻击的连锁反应 4196.2.3 修改ID的欺骗入侵 4266.2.4 ClassID与UserID两个值的欺骗 4326.2.5 简单用户名的欺骗 4366.3 Cookie欺骗攻击的多样性 4386.3.1 巧刷投票, Cookie欺骗的利用 4386.3.2 Cookie欺骗制作的手机短信炸弹 444第7章 网站成帮凶, 嫁祸攻击的跨站技术 4517.1 攻击来源于一段被写入的代码 4517.1.1 有漏洞的测试网页 4527.1.2 一个典型的动网跨站攻击示例 4557.1.3 Cookie的盗取——跨站入侵检测演示之一 4577.1.4 私服网站挂马——跨站入侵检测演示之二 4617.2 一句留言, 毁掉一个网站 4667.2.1 MM\_validateForm未过滤, YEYI的跨站检测 4667.2.2 时代购物系统的跨站入侵检测 4737.3 圈地谁为王——从Q-Zone攻击看跨站技术的演变 4777.3.1 不安全的客户端过滤 4787.3.2 编码转换, 继续跨站 4857.3.3 Flash跳转, 跳出跨站 4887.3.4 Flash溢出跨站 4937.3.5 链接未过滤, 音乐列表跨站 4957.3.6 外部调用跨站, QQ业务索要的漏洞 5007.4 邮件中不安全代码, 邮箱跨站挂马 5027.4.1 由QQ邮箱看邮件跨站危害 5037.4.2 国内主流邮箱跨站漏洞一览 5097.5 “事件”出了漏子, 主流博客空间跨站检测 5167.5.1 不需要的跨站, 标记事件属性与跨站 5167.5.2 百度空间的跨站演变 5177.5.3 Onstart事件引发的网易博客跨站 5247.6 “搜索”, 跨站攻击最泛滥之地 5267.6.1 国内主流搜索引擎跨站 5267.6.2 利用网页快照进行特殊跨站 5387.7 跨站脚本攻击的终极防范 546第8章 打造安全的网站服务器 5518.1 配置安全的Web服务器 5518.1.1 删除不必要的IIS组件 5518.1.2 IIS安全配置 5538.2 数据库的安全防护 5578.2.1 Access数据库防下载处理 5578.2.2 SQL数据库的配置 5598.3 对网页木马后门的防范和检测 5618.3.1 删除各种脚本对象以禁止ASP木马运行 5618.3.2 网页木马后门查找工具 5648.3.3 设置网站访问权限 565

<<网站入侵与脚本攻防修炼>>

章节摘录

插图：

## <<网站入侵与脚本攻防修炼>>

### 编辑推荐

《网站入侵与脚本攻防修炼》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。

Web入侵揭秘。

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。

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。

<<网站入侵与脚本攻防修炼>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>