

<<揭秘Web应用程序攻击技术>>

图书基本信息

书名：<<揭秘Web应用程序攻击技术>>

13位ISBN编号：9787508464497

10位ISBN编号：7508464494

出版时间：2009-5

出版时间：水利水电出版社

作者：王继刚

页数：288

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>

## <<揭秘Web应用程序攻击技术>>

### 前言

2008年5月29日，陕西省地震信息网遭受到了恶意的黑客攻击，在陕西省地震信息网“四川汶川8.0级地震应急”栏目中赫然出现了一则关于“23时30分陕西各地会有强烈地震发生”的虚假信息 and 一条题为“网站出现重大安全漏洞”的警告信息。

相继陕西省地震信息网被恶意攻击后，广东省地震信息网也遭到恶意攻击，甚至连四川重灾区的地震信息网也被非法入侵者破坏，这些网站都是属于国家机关的政府网站，在汶川大地震这样举国悲痛的时刻，竟然有人利用自己的一点黑客技术去在陕西省地震信息网上恶意散布地震谣言，蛊惑人心，究竟是什么动机让这些“网络黑客”做出如此令人发指的事情呢？

静下心来思考，除去那些破坏者扭曲的心理，作为网站核心的Web应用程序本身漏洞重重，加上网站管理人员脆弱的网络安全意识，这才会让攻击者有机可乘，网络安全的警钟再一次对我们每一个人敲响。

后来，有新闻记者采访了其中一位被公安机关抓获的网络攻击者，当问到他是利用什么技术攻击网站的时候，这位所谓的“黑客”说道：“其实也没有什么，那个网站的漏洞太明显了。”

一句简单的回答，对于一个普通的人来说太令人感到困惑，究竟这些黑客到底是怎样找出网站上Web应用程序中的漏洞，又是怎样利用这些漏洞攻击网络服务器的，这些问题都是一个谜。

而对于那些维护网站安全的管理人员来说，他们更渴望知道他们的程序究竟在哪里出现了问题，自己怎样做才能防止此类事情再度发生，防患于未然。

正因为如此，我决定写一本书，来揭开这些隐藏在黑暗深处的秘密，不再让我们感到谈“黑”色变。本书写作思路不同于以往的安全书籍，在这里没有采用教科书式的纯理论化介绍，而是将实际的讲解实例全面介绍给读者。

本书也没有用那些属于老黄历的过时技术来进行凑数，而是将现在最流行的网络程序攻击技术拿出来与读者一起学习。

在将这些攻击技术原理讲清楚的同时，把如何发掘Web应用程序安全漏洞的方法也一并说出来，这样做的目的是让每一位阅读本书的读者能够全方位了解Web应用程序安全的始终。

本书也第一次让读者真实地扮演一位Web应用程序的“攻击者”，从分析目标程序漏洞开始，一步步带领读者走进神秘的黑客世界。

让每一位阅读本书的读者切切实实地明白Web应用程序的安全现状。

本书在讲述网络程序如何被“黑”的同时，更加注重将如何防范Web应用程序被“黑”的安全经验告诉读者，让读者能够对这两者都有一个兼顾学习。

Web应用程序的安全漏洞就像是计算机病毒，如果我一直告诉你安装某某杀毒软件就可以防止病毒入侵，那么当你安装了杀毒软件却又中毒的时候，你很可能就不会再相信我说的任何话；相反，如果我告诉你什么是计算机病毒、计算机病毒之所以产生的原理，以及如何全面防范被病毒感染，那么即使你下一次又中毒了，你会说这其实并不可怕，因为你知道如何对付这些病毒。

## <<揭秘Web应用程序攻击技术>>

### 内容概要

互联网安全已经深入影响到当今社会的每一个角落，网络犯罪、网络恶意攻击几乎时时刻刻都在上演，而导致这些问题发生的最大安全隐患正来自于网络的核心——web应用程序。

本书以实例与理论相结合的方法，带领读者一同进入Web应用程序安全领域，让读者亲身扮演一位安全研究人员，从认识Web应用程序、理解Web结构开始，一步一步进入Web应用程序的漏洞分析及攻击技术剖析。

本书详细讲述了各种Web应用程序攻击技术的分类及来由，第一次为读者揭开了Web应用程序漏洞的发掘技术，同时，列举了许多真实的Web应用程序攻击案例，供读者参考。

本书适合所有热爱网络安全的人们，尤其是高等院校计算机专业的学生。

同时，本书可作为计算机安全培训班及学校教材和参考书籍，也为Web应用程序开发人员及网络管理人员提供了不可多得的安全参考资料，有很高的实用价值。

## 书籍目录

前言第1章 脆弱的Web应用程序 1.1 所谓的“安全” 1.2 定义Web程序安全漏洞 1.2.1 漏洞的概念 1.2.2 漏洞的特性 1.2.3 系统的信任等级 1.2.4 漏洞与系统攻击之间的关系 1.2.5 Web应用程序安全漏洞的引入 1.3 Web程序漏洞的分类 1.4 引发漏洞的始因 1.5 Web漏洞攻击的趋势 1.5.1 蠕虫化 1.5.2 病毒化 1.5.3 恶意化 1.5.4 Oday化第2章 基础知识 2.1 Web——世界的奇迹 2.1.1 什么是Web 2.1.2 Web运行原理 2.1.3 Web技术 2.1.4 Web 2.0带来的变革 2.2 Web程序的开发 2.2.1 服务端开发语言 2.2.2 客户端开发语言 2.3 Web程序运行环境 2.3.1 常见的Web Servet 2.3.2 Web Server与服务器系统 2.3.3 状态码 2.4 Web程序的数据通信 2.4.1 HTTP / HTTPS协议 2.4.2 Cookies的作用 2.4.3 GET与POST数据提交 2.5 Web应用程序数据加密方式 2.5.1 MD5加密 2.5.2 URL Encode 2.5.3 Base64加密第3章 搭建攻击平台 3.1 发掘工具的准备 3.1.1 浏览器 3.1.2 编码工具 3.1.3 监视工具 3.1.4 调试工具 3.2 虚拟机 3.2.1 虚拟机的概念 3.2.2 VMware的安装使用 3.3 安装Web程序运行环境 3.3.1 IIS环境的搭建 3.3.2 XAMPP的使用 3.3.3 Tomcat的安装第4章 最广泛的漏洞——XSS 4.1 初次接触XSS漏洞 4.1.1 艺术化的XSS漏洞 4.1.2 Stored.XSS漏洞 4.1.3 DOM—Based XSS漏洞 4.2 手工发掘：XSS漏洞的方法 4.2.1 寻找关键变量 4.2.2 页面表单测试 4.2.3 反馈信息观察 4.3 传统的XSS漏洞利用 4.3.1 Cookies欺骗 4.3.2 隐蔽网页木马 4.3.3 电子邮件中的XSS攻击 4.4 无可匹敌的XSS木马 4.5 可怕的XSS蠕虫 4.6 飞天论坛XSS漏洞发掘实例 4.7 防范XSS漏洞 4.7.1 过滤与加密变型 4.7.2 客户端的防范第5章 针对数据库的攻击——SQL注入漏洞 5.1 常见的网站数据库 5.2 SQL简介 5.3 注入思想的诞生 5.4 IIS的“友好”帮助 .....第6章 通过WEB控制系统系统第7章 引用文件带来的危害第8章 堪称经典的上传漏洞第9章 Web应用程序做嗅探第10章 混乱的Web程序员第11章 渗透编译型Web程序第12章 自动化漏洞发扬技术第13章 穿透安全防范机制第14章 新起的Web程序攻击 参考文献及参考资料

## 章节摘录

插图：第1章 脆弱的Web应用程序不知道在你上网的时候，有没有看见过如图1.1所示的画面。这是一张被恶意攻击者渗透进入后的网站截图，攻击者篡改了网站的首页内容，图1-1中那挑衅的字眼似乎在告诉每一个看到它的人说：“这个网站并不安全。”

在互联网上，这些用来为广大网民提供信息服务的网站，几乎每一个时刻都在面临着如此恶意的攻击。

当网站服务器的开发者竭尽全力加强网站安全的时候，Web应用程序却成为了网络这个安全木桶上最短的一块挡板。

管理学中的木桶原理告诉我们：一个木桶由许多块木板组成，如果组成木桶的这些木板长短不一，那么木桶的最大容量不取决于长的木板，而取决于最短的那块木板。

这个原理同样适用于信息安全。

一个结构的信息安全水平将由与信息安全有关的所有环节中最薄弱的环节决定。

安全就像是水，木桶就像是需要安全保护的的网络环境，一个可以用来装水的木桶，必须保证木桶上的每一块挡板长度都要一样，不然，一旦我们想要给木桶装满水的时候，水就会从最短的那一块挡板上流出，那就意味着安全问题将会从木桶上最短的一块挡板上发生。

在本章里，我将把它作为一个引子，告诉大家为什么我们要谈论：Web应用程序的安全问题，它真的严重到我们需要整整一本书的版面来说明这个问题吗？也许，我们谁都不希望在每天打开计算机上网的时候，映入眼帘的画面全部都像图1.1那样令人不安。

至于那些具体的安全理论和方法，会在后面的章节详细讲述。

## <<揭秘Web应用程序攻击技术>>

### 编辑推荐

《揭秘Web应用程序攻击技术》特点：全面着眼于Web应用程序安全，解密当今流行的黑客攻击技术内幕；精选安全案例，深入浅出讲解Web应用程序安全漏洞的发现与利用；了解Web安全的实质，学会有效的防范技术，真正带领读者走近Web应用程序安全研究者的神秘领域。

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>