Web Security & Commerce

Web 安全与电子商务

O'REILLY®
中国电力出版社

Simson Garfinkel, Gene Spafford 著
何健辉 刘祥亚 冯延晖 译

Web安全与电子商务

Simson Garfinkel with Gene Spafford 著

何健辉 刘祥亚 冯延晖 译

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

O'Reilly & Associates, Inc. 授权中国电力出版社出版

中国电力出版社

图书在版编目（CIP）数据

Web安全与电子商务 /（美）加丰凯尔（Garfinkel, S.）等编著；何建辉等译．
-北京：中国电力出版社，2001

书名原文：Web Security & Commerce

ISBN 7-5083-0715-1

Ⅰ.W... Ⅱ.①加... ②何... Ⅲ.①万维网－安全技术 ②万维网－电子商务 Ⅳ.TP393.4

中国版本图书馆CIP数据核字（2001）第051162号

北京市版权局著作权合同登记

图字：01-1999-3750号

书　　名/ Web安全与电子商务

书　　号/ ISBN 7-5083-0715-1

责任编辑/ 刘敏

封面设计/ Edie Freedman，张健

出版发行/ 中国电力出版社（www.infopower.com.cn）

地　　址/ 北京三里河路6号（邮政编码100044）

经　　销/ 全国新华书店

印　　刷/ 北京市地矿印刷厂

开　　本/ 787毫米×1092毫米　16开本　31.5印张　460千字

版　　次/ 2001年9月第一版　2001年9月第一次印刷

印　　数/ 0001-5000册

定　　价/ 59.00元（册）

Web 安全与电子商务

O'Reilly & Associates公司介绍

为了满足读者对网络和软件技术知识的迫切需求，世界著名计算机图书出版机构O'Reilly & Associates公司授权中国电力出版社，翻译出版一批该公司久负盛名的英文经典技术专著。

O'Reilly & Associates公司是世界上在UNIX、X、Internet和其他开放系统图书领域具有领导地位的出版公司，同时是联机出版的先锋。

从最畅销的《The Whole Internet Use's Guide & Catalog》（被纽约公共图书馆评为二十世纪最重要的50本书之一）到GNN（最早的Internet门户和商业网站），再到WebSite（第一个桌面PC的Web服务器软件），O'Reilly & Associates一直处于Internet发展的最前沿。

许多书店的反馈表明，O'Reilly & Associates是最稳定的计算机图书出版商——每一本书都一版再版。与大多数计算机图书出版商相比，O'Reilly & Associates公司具有深厚的计算机专业背景，这使得O'Reilly & Associates形成了一个非常不同于其他出版商的出版方针。O'Reilly & Associates所有的编辑人员以前都是程序员，或者是顶尖级的技术专家。O'Reilly & Associates还有许多固定的作者群体——他们本身是相关领域的技术专家、咨询专家，而现在编写著作，O'Reilly & Associates依靠他们及时地推出图书。因为O'Reilly & Associates紧密地与计算机业界联系着，所以O'Reilly & Associates知道市场上真正需要什么图书。

目录

第五部分 Web 服务器安全

第六部分 商业贸易与社会交际

第七部分 附录

前言

1996年8月17日，一个星期六的早晨，美国司法部的一个计算机系统遭到了袭击。被袭击的目标是司法部的Web服务器*www.usdoj.gov*。袭击者破坏了它的安全防范系统，并修改了它的主页——加上了纳粹德国的国徽、猥琐的图片以及对通信风化法案的诽谤（具有讽刺意味的是：该法案最近被费城的一个联邦法庭宣布为违反美国宪法）。

当FBI技术人员发现这个被损毁的Web站点并拔掉插头时，它已在Internet上保留了几个小时。接下来由于司法部没有备用的服务器，因此当人们尝试访问司法部的主页时，均一无所获。

这次事件使得司法部在国际电台、电视以及美国报刊等公开场合均处于尴尬的境地。后来司法部承认：对于Web服务器的安全性，他们并没有给予太多的关注。因为这个服务器并没有存放任何机密信息。毕竟，这个Web服务器仅仅存放公众可以获取的有关该部门自身的一些信息，而非有关正在调查的机密信息。

通过Web，司法部可以利用革命性的新方法向公众发布信息——该系统在降低费用的同时，还可以使信息更容易被获取。但显然这次袭击说明这台Web服务器上的信息不能被保密。由于这台Web服务器是司法部公开面向网上世界的一扇窗口，因此允许它被改变就等于破坏了司法部的声誉。

无独有偶，1996年9月18日，一群瑞典黑客闯入了美国中央情报局（CIA）的Web站点（*http://www.odci.gov/cia*）。中情局的反应与FBI一样：首先拔掉插头，然后

检查系统。几个月后，美国空军的主页上也发生了类似的事件，国防部关闭了所有可从外部登录的Web服务器，花了几天时间来确保服务器的安全性并修补缺陷。

1997年3月3日，星期一，一种全新的网络威胁崭露头角。Worcester理工学院的学生Paul Greene，发现了一种特别编写的网页，它能够通过目标计算机上的任意输入来骗得在Microsoft的IE浏览器上执行任何程序。一个袭击者可以用这个bug去捣毁一台计算机，可以用病毒感染它，也可以从它的硬盘上获取私人信息。这个bug还能使得网络管理员完全控制任何一台用IE访问其Web站点的计算机。

48小时之内，Microsoft就在其Web站点上发布了针对Greene发现的bug的补丁程序，显示出了该公司的反应能力，以及网络在发布bug的补丁程序时的高效率。但还是在这一星期，人们又在IE浏览器中发现了另外一个同样具有潜在危险效应的巨大缺陷。同样的问题不仅仅发生在Microsoft身上：在同一星期，别的研究人员在使用Netscape公司的Navigator浏览器时，在Sun公司的Java环境中也发现了一个新的bug。

Web：希望与威胁

司法部、空军和CIA都是幸运的。因为尽管这些入侵对于他们而言都是一种公开的耻辱，但这些机构的Web服务器上都没有存放任何机密信息。几天以后，这些系统又重新运转起来。这次，我们希望安全问题会得到保障。但事实并非如此。Microsoft以及成千上万的IE用户也是幸运的，因为尽管IE的bug被大肆渲染，但并没有导致大范围的数据丢失。

现在反政府的黑客不再是采取强硬的入侵手段，而是采用一种秘密的入侵方式。他们用一台中间计算机作为跳板来袭击政府的其他机器。或者，他们仅仅对网页做一些细微的改动 —— 例如，改变电话号码，伪造令人难堪的引用语，或者只是在这个网站上放置一些暗含诽谤或指向其他被更改的网页的信息。这些袭击者还可以安装软件来窥探该组织的网络，以帮助他们入侵其他更机密的机器。

在*www.usdoj.gov*遭到入侵的前几天，马萨诸塞州州政府宣布，驾驶员可以在Web上支付他们的超速罚款单及其他违反交通规则的罚单。他们仅仅需要访问机动车辆登记处的网站，点击几个链接，就可以用一张信用卡来支付超速罚单了。该州一位官员说："与排队支付罚款相比，我们相信公众更愿意在线支付。"

为了在Internet上安全地接受信用卡，机动车辆登记处网站使用了一个“安全的”Web服务器。在这里，“安全的”是指Web服务器和Web浏览器之间的连接是安全的。这意味着，Web服务器实施了某些密码协议，当一个人的信用卡号在发送时会进行编码，从而不会被中途截获。

但是，由马萨诸塞州政府管理运行的Web服务器并不比司法部的Web服务器更安全。仅仅使用密码在网络上发送信用卡号，并不意味着计算机不能被入侵。而且，如果这台计算机被入侵，其后果将远不止在公众中处于尴尬境地。袭击者们将不再满足于改变网页，他们可能会在服务器上安装软件以偷偷捕获被解码的信用卡卡号，然后利用偷取的卡号进行诈骗。要找出信用卡窃贼的藏身之处，信用卡公司往往要花费好几个月，而到那时，这些窃贼已经转向其他受害者了（注1）。

或许，下一次，这些袭击者仅仅通过放置强制性HTML代码就能够利用Netscape的Navigator和Microsoft的IE浏览器中广为人知的bug对Web服务器进行入侵了。

这些事件告诉了我们Web上既存在希望又存在威胁。Web的希望在于它能使组织机构在发布信息、产品以及提供信息的时候，极大地降低成本。而威胁则在于：计算机构建成的网络都是脆弱的，它们能够而且已经被损害过。更糟糕的是：随着Web的应用越来越广泛，会有更多重要的组织机构上网，从而会有更多的人使用它，结果会使这些计算机成为引人注目的攻击对象。

1997年，美国Strategic Focus公司（加利福尼亚州Milpitas的一家咨询公司）对400位信息系统经理进行了调查，结果表明，对那些准备在网上开展业务的公司来说，安全性是他们最担心的问题。这个公司的总裁Jay Prakash说：“对于任何一种电子商务而言，安全性都是让人最关心的问题，而且这种情况会持续一段时间”。他还发现，在被调查的公司当中，有55%的公司存在安全隐患。

关于本书

这是一本有关Web安全及电子商务的书。本书主要展示处于网络世界中的人们所面临的威胁，并提供减少这些威胁的方法。

注1：我们并不是暗示马萨诸塞州政府的网站是不安全的，而只是用它作为一个例子来说明基于Web的应用存在风险。发生在饭店、传统的邮购公司的信用卡诈骗都是确有其事，而基于Internet的诈骗则给了骗子和罪犯更新的、更有利的机会。

本书是为使用Web浏览器在Internet上获取信息的个人，以及使用Web服务器提供数据和服务的组织机构而编写的。它包括对基于Internet的计算机安全性问题的概述，许多章节还阐述了为促进Internet的商业化而产生的新协议和产品。

在本书中，特别值得注意的是：

- 联机世界中存在的风险、威胁及益处
- 怎样控制在Web服务器上的信息存取
- 怎样减少Web服务器被攻击的机会
- 怎样使服务器在遭受到损害后能迅速恢复
- 什么是加密，以及怎样用它们来保护你的用户和系统
- 由于使用Java、JavaScript、ActiveX以及Netscape的插件而产生的安全问题
- 一些值得讨论的法律问题

本书涵盖了Web安全的基本问题，但它并不是一本计算机安全、操作系统或Web的初级读物。因此，我们推荐了许多其他由O'Reilly & Associates公司出版的好书。其中包括Eleen Frisch的《Essential System Administration》、Chuck Musciano和Bill Kennedy的《HTML: The Definitive Guide》、Shishir Gundavaram的《CGI Programming on the World Wide Web》、Deborah Russell和G.T的《Computer Security Basics》，以及我们编写的《Practical UNIX & Internet Security》。有关密码学的进一步的探讨请参考Bruce的《Applied Cryptography》（由John Wiley & Sons出版，译注1）。

章节介绍

本书共分7部分，包括19章和5个附录。

第一部分：概述，介绍连接到Internet上的计算机安全方面的基础知识。

译注1：以上推荐的书籍有许多已经由中国电力出版社推出了中文版本。感兴趣的读者请访问中国电力出版社的网站：*www.cepp.com.cn*。

第一章“Web安全状况”。本章简短地回顾了Web安全的历史，介绍了有关Web安全方面的术语，同时阐释了一些在Web上开展业务时可能面临的风险。

第二部分：用户安全，指出用户使用不同浏览器时将会面临不同的风险，提供了当前使用最广泛的两种浏览器（Microsoft的IE与Netscape的Navigator）的相关信息。这部分内容主要面向一般用户。

第二章“有Bug的浏览器：风险的形式”。本章阐述了浏览器的发展史，探讨了其中最大的威胁：因粗心、草率地使用而带来的错误。

第三章“Java和JavaScript”。本章探讨了由Java和JavaScript带来的安全风险。

第四章“用ActiveX和插件下载机器代码”。本章探讨了在计算机上运行随机代码所带来的严重危险。

第五章“个人隐私”。本章探讨了在线隐私权、Cookie技术以及秘密泄露的问题。

第三部分：数字认证，阐释了什么是数字认证，以及如何通过使用数字认证来在Web上建立身份和信用。

第六章“数字认证技术”。本章阐释了怎样用密码学来确认在联机环境中的身份。

第七章“认证机构和服务器证书”。本章给出了对特定的各种用来建立Web服务器的身份的数字认证的实际观点。

第八章“客户端数字证书”。本章讨论了用来在Web上建立身份的数字认证的正、反两方面情况。

第九章“代码签名与Microsoft认证码”。本章阐释了怎样用数字认证来签署可执行文件，以及这些签名是怎样被确认的。

第四部分：密码学，给出了密码学的一个整体说明，并讨论了它是如何适应当今网络发展的。这部分内容对于那些对Web出版和商业感兴趣的个人或组织是非常有用的。

第十章“密码学基础”。本章讨论了加密及其消息摘要所扮演的角色。

第十一章“密码学和网络”。本章讨论了密码在Internet加密方面所扮演的角色。

第十二章“理解SSL和TLS”。本章介绍了安全套接字层以及传输层安全协议的概况。

第五部分：Web服务器安全，研究了保障Web服务器安全的技术。

第十三章“主机和网站安全”。本章包括有关UNIX系统和Windows NT（注2）的各方面的安全。

第十四章“控制对Web服务器的访问”。本章讨论了怎样才能通过建立在Web服务器内部的访问控制系统，来严格控制一个Web服务器提供给特定用户的信息。

第十五章“安全的CGI/API编程”。本章讨论了在编写CGI脚本以及利用Web服务器的API时所面临的安全问题。

第六部分：商业贸易与社会交际。本章探讨了Web上涉及金钱与社会的关键问题。这部分内容是一般读者所感兴趣的。

第十六章“数字支付”。本章探讨了在线支付的方式。

第十七章“审查软件和审核技术”。本章介绍了控制利用Internet进行访问时所使用的技术。

第十八章“民事法律条款”。本章探讨了在Web上发布信息所涉及的民事法规。

第十九章“刑事法律条款”。本章探讨了Web内容导致的刑事问题。本章是第十八章的继续。

第七部分：附录，包括总结和技术信息。

附录一“来自于Vineyard.net的教训”。本附录是一个有关建立及运营Internet服务提供商的个人报道，报道中还包括有关尝试确保其安全性的问题。

附录二“建立和安装Web服务器认证”。本附录展示了Apache-SSL Web服务器的

注2：目前Web服务器主要是在这两种操作系统上运行的，而且它们都面临着安全性方面的极大挑战。