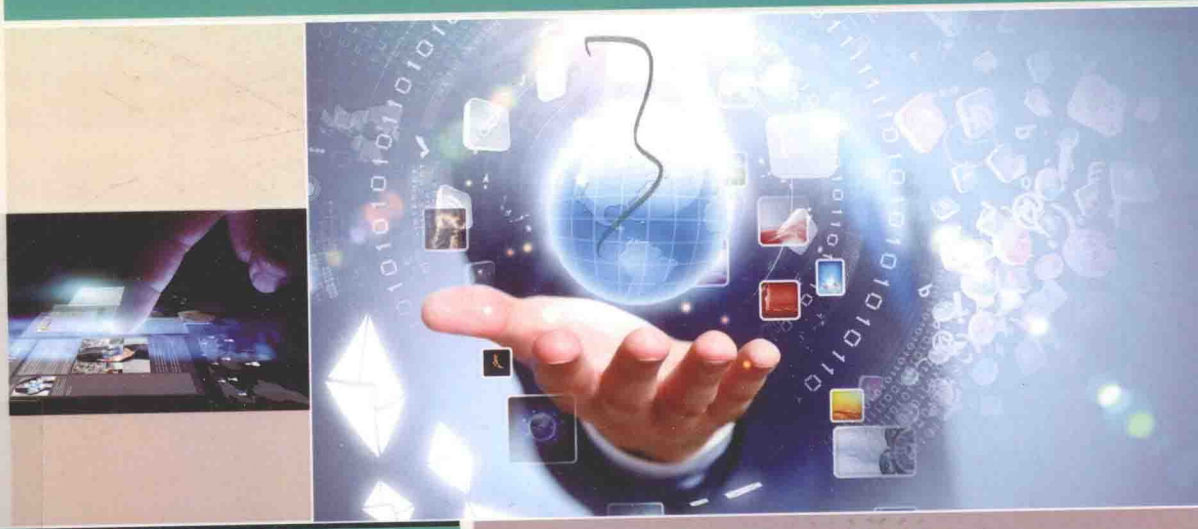
高等院校电子商务专业系列规划教材

电子商务安全

（第2版）



DianZI ShangWu AnQuan

刘英卓　主编

中国工信出版集团

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

电子商务安全

（第2版）

DianZI ShangWu AnQuan

刘英卓　主　编
曹　杰　张艳萍　副主编

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

图书在版编目（CIP）数据

电子商务安全 / 刘英卓主编. —2 版. —北京：电子工业出版社，2016.7
高等院校电子商务专业系列规划教材
ISBN 978-7-121-29143-2

Ⅰ. ①电… Ⅱ. ①刘… Ⅲ. ①电子商务—安全技术—高等学校—教材 Ⅳ. ①F713.36

中国版本图书馆 CIP 数据核字（2016）第 140331 号

策划编辑：姜淑晶
责任编辑：李慧君
印　　刷：北京嘉恒彩色印刷有限责任公司
装　　订：北京嘉恒彩色印刷有限责任公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1 092　1/16　印张：21.5　字数：523 千字
版　　次：2010 年 7 月第 1 版
　　2016 年 7 月第 2 版
印　　次：2016 年 7 月第 1 次印刷
定　　价：43.00 元

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）88254888，88258888。

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。

本书咨询联系方式：（010）88254199，sjb@phei.com.cn。

前　言

未来的商务必将成为完全的电子商务，未来的经济也必将是网络化的经济，这是科技的应用和发展之必然。电子商务进一步强调了同一个地球的概念，给整个世界带来了交易上的大一统。但任何事物的发展都存在着两面性，数分实虚、词分实虚、意分显隐，矛与盾一直在相辅相成中伴随着事物发展。电子商务一直存在安全的主题，安全问题解决好了，将会更大限度地释放电子商务的经济效能。

本书是《电子商务安全与网上支付》一书的改进版，不再讲解网上支付的相关知识，而将核心完全转移到电子商务安全上来。一是为配合开设课程，二是使内容更精准。本书的调整之处主要有：将每章的引导案例做了改写，目的是使案例更具时代性、更符合章节内容；增加了 AES 算法的讲解，目的是适应国际安全形势；更新了书中比较陈旧的内容，如当前主流操作系统为 Windows Server 2008，所以对相关内容均做了调整；增加了安全电子商务编码一章，一是让学生贯通理论到现实的逻辑思维转换，二是顺承所开设的 Java 课程对 Java 安全知识的运用；书后增加了附录，附录有助于教师和学生理解书中相关知识。

本书面向高等院校中的电子商务本科学生；也可供 MBA、经济管理类专业硕士选用；还可供相应层次的电子商务安全人员培训时选用。

本书编写的目的是充当教材，教材必须具有教师教而传授给学生的“材”，还必须有适合学生学习的“材”。因此，一本好的教材要安排好内容的质和量。质上要让学习者能够学习到东西、讲授者能够方便讲授，这就需要调整好知识点、知识面和知识体。量上要考虑一学期、一节课的知识量在章节中的合理安排。我们常常发现，有很多被称为教材的书，里面充斥了大量东拼西凑、四处网罗来的阅读资料，篇幅极为厚重，但教师看了不知其所教，学生看了不知其所学。本教材的特点是：一定的基础知识的导引，一定的故事趣味性，一定的知识深度，一定的应用实例；语言简洁明了，知识点突出，层次分明；注意课程间的衔接和深入。

通过本书的学习，能够使学生全面了解计算机信息安全技术的基础理论，初步掌握计算机信息安全防范的基本方法，加强对计算机安全重要性的理解，掌握实现和管理 Windows

Server 网络环境的知识和技能，具备进行故障排除的能力。为学生今后进行进一步学习、研究信息安全技术打下坚实的基础。

本书由刘英卓、曹杰和张艳萍编写，刘英卓负责编写书中正文内容，张艳萍编写了引导案例和实验内容及习题内容，曹杰做了全书的审阅和校对工作。本书尽量保留了作者认为重要的、有实用价值的或者有趣的内容，注意了和同类教材内容上的区分。在教材编写过程中，参考了国内外有关的最新著作和资料，南京财经大学电子商务实验室的相关老师也提出了宝贵的建议，在此表示衷心的感谢！由于作者的水平和教学经验有限，书中难免有不足之处，希望广大读者批评指正。

教学建议如下表。

	知识点	课时安排	重点讲述内容	选讲内容
第1章	电子商务安全的基本知识点，客户机的安全，服务器的安全，安全的目标，安全的威胁等	4课时	客户机的安全设置；服务器的安全原理和设置	安全评估标准
第2章	加密和解密基本知识，DES算法原理，AES算法，RSA算法	6课时	DES算法、RSA算法	AES算法
第3章	TCP/IP基本知识，IPSec协议、SSL协议和SET协议	8课时	TCP/IP基本知识，IPSec原理，SSL协议，SET协议	IPv6，VLAN
第4章	防火墙和VPN基本知识	8课时	防火墙基本原理、VPN 原理	GRE VPN和MPLS VPN
第5章	鉴别和认证基本知识	6课时	鉴别和认证基本原理，PKI和CA	域与活动目录
第6章	安全策略和安全实践	3课时	安全策略和安全实践注意事项	电子商务安全案例
第7章	安全电子商务编码	10课时	Java安全，JSP安全，购物车的实现	数字签名
第8章	安全的网上支付	3课时	在线支付功能的安全实现	中国金融认证

本建议表是按照一学期18周、每周3课时、2次复习课来设计的，仅供教师使用时参考。每一本书都在面临着内容的老化，即使最新的书也是难免的。所以，广大教学者和学习者在使用本书时，请及时更新本书中已经过时的数据，欢迎对本书中的不当之处提出指正。

目 录

第 1 章

电子商务安全概论

引导案例

2012 年 5 月 29 日，工业和信息化部计算机与微电子发展研究中心（中国软件测评中心）等部门发布的《网站用户口令处理安全性外部测评报告》指出，在 100 个样本网站中，淘宝、京东、携程、世纪佳缘等 85 个网站可在服务器端获取用户口令原文，仅 8 家网站采取了最安全的用户口令传输模式。大部分样本网站在传输口令时，没有做加密处理。其中，12 家电子商务网、15 家招聘网、10 家婚恋网站采用了最不安全的“原始口令明文传输”，对口令没有采取任何技术手段加密。一般而言，用户在登录网站，输入用户名和密码之后，从用户电脑传输到网站服务器，会经过口令传输、口令存储认证等过程。用户名和密码通过管道到达网站服务器，如果运营商铺设的管道安全，尚可抵御外部攻击；如果用户本身所在的网络是不安全的，比如在私人建设的 WiFi 网络中，处在同一网段内的黑客，就可以通过简单的网络嗅探或企业间谍等工具获取用户密码信息。即便用户密码设置得再复杂，也是形同虚设。网站对用户口令安全性进行维护其实不难，之所以出现各种疏漏，可能还是网站安全意识不够。对于用户来说，用一个密码“包打天下”是非常危险的。

◇ 本章学习目标 ◇

1. 了解和掌握造成客户机和服务器安全问题的原因；
2. 掌握如何保护 PC（个人计算机）的安全；
3. 掌握电子商务的安全目标；
4. 学会如何配置安全的 Web 服务器。

在开放式网络上发展电子商务，运行 B2B、B2C 和 C2C 等电子商务模式，首先需要关注的问题是电子商务的安全性，人们对隐私、产权和钱财等是否能够得到安全保障的担心制约了电子商务的发展。国外发达国家由于在芯片和信息安全技术的应用上起步较早，因而在

相关安全产品的研发和应用方面处于领先地位。由于缺乏自主的计算机网络核心技术和软件、安全意识淡薄、防范机制不完善、法律法规不健全、缺乏电子商务安全管理专业技术人才，所以我国的电子商务发展尤其受到安全问题的制约。由于电子商务主要是利用网络来进行商务业务往来的处理和管理的，所以按照实施电子商务的对象可以划分为3个部分：客户机的安全、通信信道的安全和服务器的安全。按照技术和应用的区别，又可以将电子商务的安全分为电子商务网络安全和电子商务交易安全。

1.1 客户机的安全

客户机是指一台连接远程服务器的本地机，通常是PC，也是B/S结构中的浏览器一端。其安全性可划分为两段：客户机上网前的安全和客户机上网后面临的安全。对于客户机上网前的安全，主要是其硬件、软件的安全问题，硬件方面有计算机的各种插卡有没有问题，是否做到了功能统一、相互匹配，以及对意外事件的抵御能力等；软件方面有操作系统是否及时更新了漏洞，各种应用软件有没有被入侵的风险等。这种客户机上网前的安全性是电子商务安全的前提，要求必须首先实现PC的安全。客户机上网后面临的安全，是指客户机和服务器进行信息往来传送时面临的被攻击问题，是电子商务安全的主要关注点。

客户机上网面临的安全性问题主要来源于页面的活动内容。活动内容是指在页面上嵌入的对用户透明的程序。活动页面可显示动态图像、下载和播放音乐或利用插件来执行相关功能模块，使页面功能更为丰富、形式更为活泼。活动内容形式包括Java小应用程序、Active X控件、浏览器插件、JavaScript、VBScript、活动脚本和包含一些隐含嵌入指令的文件等。小应用程序是可以在另一个程序中执行的程序，但它不能在计算机上直接执行。只要客户的浏览器兼容Java，Java小应用程序就可以在客户机上运行。Java利用Java运行程序安全区来限制Java小应用程序的活动，Java运行程序安全区是根据安全模式所定义的规则来建立的，这些规则适用于所有不可信的Java小应用程序。可信的Java小应用程序是从本地文件系统中下载的，或者带有可信第三方的数字签名。插件是用于解释或执行嵌入下载图形、声音或其他对象中的指令。JavaScript和VBScript都支持页面设计者创建在浏览器端可执行的活动内容，但这种程序或页面要经过客户的手动启动。Active X是一个对象（称作控件），它由页面设计者放在页面里来执行特定任务的程序，只能运行在微软的Windows操作系统上，并要求浏览器支持Active X控件。浏览器下载到嵌有Active X控件的页面时，会提醒你是否安装执行。Active X控件一旦执行，就能访问所有的系统资源。所有形式的活动页面都支持WWW页面完成一些特定的任务。例如，网页的表单（form）或表格（table）上的按钮可激活嵌入的程序来计算和显示信息，或将客户机上的数据发给服务器。

Java Applet的下载执行过程，如图1.1所示。

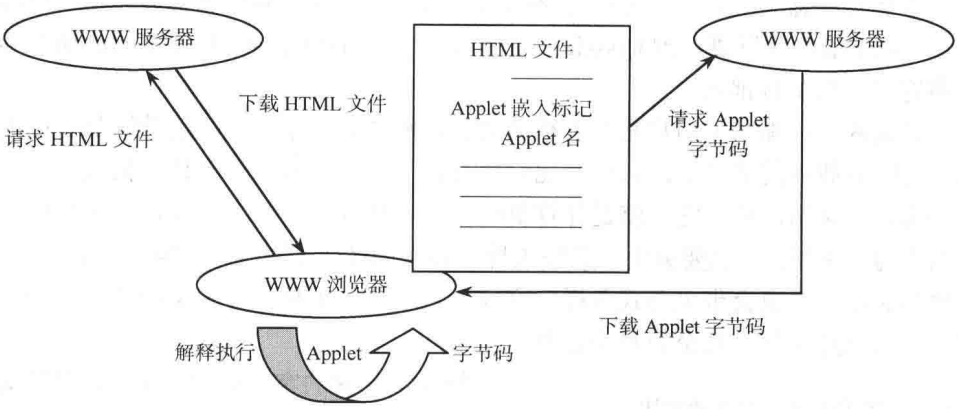


图 1.1　Java Applet 的下载执行过程

ASP 文件的处理，如图 1.2 所示。ASP.NET 文件的处理，如图 1.3 所示。

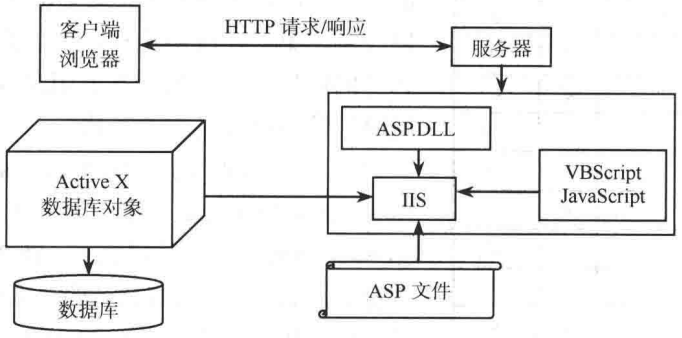


图 1.2　ASP 文件的处理

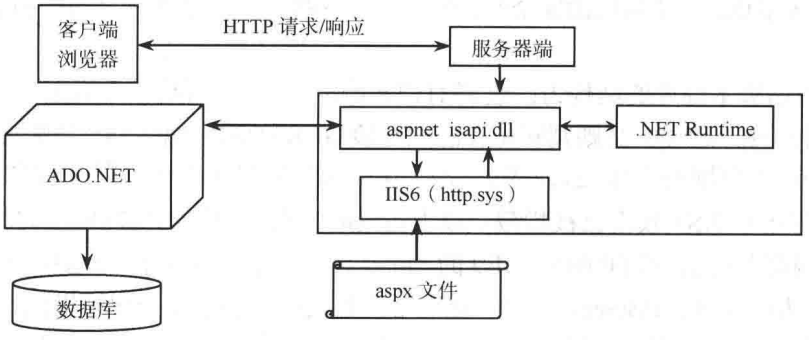


图 1.3　ASP.NET 文件的处理

如果活动内容是特洛伊木马、网络蠕虫等病毒，就将为电子商务带来多种安全风险。HTTP 协议是无状态的，即它不能记忆从一个页面到另一个页面间的响应，所以它要借助于一种叫做 Cookie 的技术来解决记忆客户订单信息或用户名与口令等问题。Cookie 是用户在访问某些站点时，其 Web 服务器在用户计算机中所写入的一些文件。这些小文件可能记录了

关于用户的个人信息，比如，何时访问该网站，在网站从事过哪些活动等。当用户再次访问该网站时，Web 服务器只要查询 Cookie 的记录就会记得用户是谁。有恶意的活动内容会利用 Cookie 将客户机的文件泄密。

除了活动内容，那些被用户有意下载的文件、软件、电子邮件的附件等都有可能带来安全隐患，这些下载后的文件中都有可能包含病毒、木马等。对每一台计算机来说，最大的两个威胁是病毒和蠕虫，其实它们就是计算机程序，有些人出于好玩或好奇而编写这些程序，有些人则作为一项挑战，想要编出最具毁灭性的病毒或蠕虫。虽然有些病毒和蠕虫完全无害，但大多数的病毒和蠕虫会带来各式各样的麻烦，从在屏幕上显示无意义的信息，到让键盘工作反常，以致删除文件，甚至使整个硬盘发生紊乱。

表 1.1 IE8 和 IE9 安全功能对比

	IE8	IE9
SmartScreen 筛选	√	√
下载声誉		√
SmartScreen URL 声誉的改进		√
InPrivate 浏览	√	√
InPrivate 筛选	√	√
选项卡隔离和恢复	√	√+
跨站脚本筛选	√	√+
点击劫持保护	√	√
域名高亮	√	√
用户首选项保护	√	√
跨站请求	√	√

如何保护上网的客户机呢？第一，对活动页面的活动内容要有所限制，设置好用户的浏览器安全选项；如图 1.4 所示是微软的 Internet Explorer9（以下简称 IE9）浏览器的 SmartScreen 应用程序声誉服务功能。第二，对活动内容喜欢访问的 Cookie，用户要加以控制。第三，对用户有意下载的文件、软件和电子邮件的附件等，要进行签名消息或签名代码的检查，同时用防病毒软件查杀病毒。

据来自 NSS Labs Web Browser Security Socially-Engineered Malware Protection（http://www.nsslabs.com/browser-security）的数据显示，在 2010 年 10 月对各种浏览器拦截社会化恶意软件的拦截率测试中，IE9 的拦截率达到 99%，排在首位。IE9 的安全考虑包括 6 个方面：隐私首选项、安全区域、数字证书、内容分级、用于 Microsoft 虚拟机的基于权限的安全性、SmartScreen 筛选。表 1.1 显示了 IE8 和 IE9 在安全功能上的对比。

IE9 对跨站脚本筛选的结构为：收到 HTTP 响应，① 判断是否导航至 HTML？② 是则判断是否为相同站点？③ 是则判断是否匹配经验 GET/POST 数据？④ 是则为每个经验匹配构建签名。⑤ 再判断响应体是否匹配签名？⑥是則對每個簽名匹配刪去適當的字符。⑦ 记录结果并通知用户 XSS 攻击已被拦截。以上诸判断若有“否”的情况则连同⑦一起转向⑧。⑧ 向 Web 浏览器提供 HTTP 响应。IE9 的 SmartScreen 筛选器可针对未知声誉的网站请求反馈。如图 1.4 所示，SmartScreen 阻止页面为用户避免已知的不安全网站提供指导。当用户通过 IE9 下载程序后，程序的文件标识以及发布者被发送到 SmartScreen 应用程序声誉服务，IE9 会据此给用户提出处理建议。

IE9 的 InPrivate 浏览方式能够有效保护用户的信息不被泄露，InPrivate 还能进行筛选和跟踪保护。表 1.2 是 InPrivate 浏览的安全效果。

图 1.4　IE 浏览器的 SmartScreen 应用程序声誉服务

表 1.2　InPrivate 浏览的安全效果

信　息	InPrivate 浏览影响效果
Cookies	驻留在内存中以确保网页工作正常，但当用户关闭浏览器时被清空
Internet 临时文件	存储在磁盘上以确保网页工作正常，但当用户关闭浏览器时被删除
网页历史记录	该信息不被存储
表单数据及密码	该信息不被存储
反钓鱼缓存	临时信息将被加密和存储以确保网页正常工作
地址栏及搜索的自动完成	该信息不被存储
自动故障恢复（ACR）	在一个会话中，ACR 能在某个选项卡崩溃时进行恢复，但如果是整个窗口崩溃了，数据将会被删除而且窗口将不能被恢复
文档对象模型（DOM）存储	DOM 存储是一种 Web 开发者可用以保留信息的“超级 Cookie”。就像普通 Cookie 一样，当窗口关闭后不会被保留

IE9 的安全性组策略可以调整，包括：限制用户更改配置；配置 SmartScreen 筛选器；限制加载项的安装和运行；确保用户不被欺骗性证书及未经签名的软件欺骗；控制哪些 HTTPS 算法被启用；针对特定网站控制哪些安全区域设置被应用；减少攻击面。

互联网是电子商务的通信信道，如何让这个信道变得安全，进行安全传输？主要包括保证互联网信道通信保密性、消息完整性和渠道可用性，互联网信道的安全性要靠各种网络协议来保障。

1.2　服务器的安全

服务器是客户机的信息资源不对等实体，它对外提供资源的共享和访问。对于电子商务的实施，建立安全的电子商务服务器系统是至关重要的。要防止服务器被破坏和非法获取信息，重点要考察其入口。服务器的入口包括 WWW 服务器及其软件、公共网关接口（CGI）程序、ASP、JSP、PL、PHP 等其他工具程序，以及任何有数据的后台程序，如数据库和数

据库服务器。

1.2.1 服务器的安全威胁

1. 对 WWW 服务器的安全威胁

WWW 服务器软件涉及的主要目标是支持 WWW 服务和方便使用，即响应 HTTP 请求进行页面传输。其面临的安全威胁主要有：

（1）WWW 服务器如果以高权限状态运行，就构成对 WWW 服务器的安全威胁，破坏者就可利用 WWW 服务器的能力执行高权限的指令。

（2）WWW 服务器如果不更改目录显示的默认设置，它的保密性就会大打折扣。如果一个服务器的文件夹名能让浏览器看到，就会破坏保密性。

（3）WWW 服务器要求输入的用户名和口令可能被泄露，Cookie 信息有可能被窃听者复制。

（4）嵌入由服务器执行的页面上的小程序会造成服务器的不安全，比如，黑客入侵网站先使用小木马开拓权限，再使用大木马全面入侵。

（5）FTP 程序会对 WWW 服务器的完整性带来安全威胁。如果没有对 FTP 用户可浏览的文件夹进行保护，就可能发生未经授权的信息泄露。

（6）存放用户名和口令的文件可能没有得到保护。

（7）用户所选的口令也会构成安全威胁。

Microsoft Active Server Pages（ASP）是服务器端脚本编写环境，使用它可以创建和运行动态的、交互的 Web 服务器应用程序。使用 ASP 可以组合 HTML 页、脚本命令和 Active X 组件以创建交互的 Web 页和基于 Web 的功能强大的应用程序。现在很多网站，特别是电子商务方面的网站，在前台上大多用 ASP 来实现，以至于目前 ASP 在网站上的应用很普遍。

ASP 脚本是一系列按特定语法（目前支持 VBScript 和 JavaScript 两种脚本语言）编写的与标准 HTML 页面混合在一起的脚本所构成的文本格式的文件。当客户端的最终用户用 Web 浏览器通过 Internet 来访问基于 ASP 脚本的应用时，Web 浏览器将向 Web 服务器发出 HTTP 请求。Web 服务器分析、判断出该请求是 ASP 脚本的应用后，自动通过 ISAPI 接口调用 ASP 脚本的解释运行引擎（ASP.DLL）。ASP.DLL 将从文件系统或内部缓冲区获取指定的 ASP 脚本文件，然后进行语法分析并解释执行。最终的处理结果将形成 HTML 格式的内容，通过 Web 服务器“原路”返回 Web 浏览器，由 Web 浏览器在客户端形成最终的结果呈现。这样就完成了一次完整的 ASP 脚本调用。若干个相关的 ASP 脚本调用就组成了一个完整的 ASP 脚本应用。

当使用 ASP 时，必须将存放.asp 文件的目录设置为“Execute（执行）”。建议在设置 Web 站点时，将 HTML 文件同 ASP 文件分开放置在不同的目录下，然后将 HTML 子目录设置为“读”，将 ASP 子目录设置为“执行”，这不仅方便了对 Web 的管理，而且更重要的是提高了 ASP 程序的安全性，防止了程序内容被客户端访问。

2．对数据库的安全威胁

把电子商务、电子贸易的着眼点集中于 Web 服务器、Java 和其他新技术的同时，应该记住这些以用户为导向和企业对企业的系统都是以 Web 服务器后的关系数据库为基础的。它的安全直接关系到系统的有效性、数据和交易的完整性与保密性。系统的延时会降低效率欠佳，不仅影响商业活动，还会影响公司的信誉。不可避免地，这些系统受到入侵的可能性更大，但是并未对商业伙伴和客户敏感信息的保密性加以更有效的防范。此外，ERP 和管理系统，如 ASPR/3 和 PeopleSoft 等，都是建立在相同标准的数据库系统中的。无人管理的安全漏洞与时间拖延、系统完整性和客户信任等问题有直接的关系。

数据库的安全威胁主要包括事务内部的故障、系统范围内的故障、介质故障、计算机病毒与黑客。其中，数据库系统故障又称为数据库软故障，是指系统突然停止运行时造成的数据库故障，如 CPU 故障、突然断电和操作系统故障。介质故障又称为数据库硬故障，主要指外存故障，如磁盘磁头碰撞和瞬时的强磁场干扰等。

（1）数据库系统的安全性要求：包括物理上的完整性、逻辑上的完整性、元素的完整性、可审计性、访问控制、用户认证、可获（用）性，如表 1.3 所示。

表 1.3　数据库系统对安全性的要求

安全问题	说　明
物理上的完整性	预防数据库数据物理方面的问题，如掉电，以及被灾祸破坏后能重构数据库
逻辑上的完整性	保持数据的结构，例如，一个字段的值的更改不至于影响其他字段
元素的完整性	包含在每个元素中的数据是准确的
可审计性	能够追踪谁访问修改过数据库的元素
访问控制	允许用户访问被批准的数据，以及限制不同的用户有不同的访问模式，如读或写
用户认证	确保每个用户被正确地识别，既便于审计追踪，也为了限制对特定的数据进行访问
可获（用）性	用户一般可以访问数据库及所有被批准访问的数据

（2）数据库系统信息安全性依赖于两个层次：一个是数据库管理系统本身提供的用户名/口令字识别、视图、使用权限控制、审计等管理措施；另一个是应用程序设置的控制管理。

（3）数据库保护：主要是指数据库的安全性、完整性、并发控制和数据库恢复。

3．公共网关接口（CGI）程序、ASP、JSP、PL、PHP 等其他工具程序的安全威胁

公共网关接口（CGI）程序、ASP、JSP、PL、PHP 等其他工具程序，都可以实现从 WWW 服务器到另一个程序的信息传输，如果滥用就会带来安全威胁。它们能够提高运行权限，以至于能自由访问系统资源；同时，它们很难追踪和管理。攻击者可能会追踪这些工具程序，检查并了解它们，然后加以利用。

4．服务器所运行程序的安全威胁

① 通过客户机传输给 WWW 服务器或直接驻留在服务器上的 Java 或 C++程序造成的缓存溢出性攻击。

② 服务器被用做攻击跳板的攻击威胁，如邮件炸弹。

1.2.2 保护电子商务服务器

电子商务服务器软件包括WWW服务器、FTP服务器、电子邮件服务器、远程登录服务器、数据库服务器、域名服务器和主机上的操作系统等。每种服务器软件都需要单独考虑制定其安全模式，还要做到整体的统一协调。

1. 商务服务器的安全解决方案

（1）访问控制和认证

访问控制和认证是指控制访问商务服务器的人和访问内容。服务器可用多种方式对用户进行认证。第一，证书是用户的许可证；第二，服务器检查证书上的时间标记以确认证书是否过期，并拒绝为过期证书提供服务；第三，服务器可使用呼叫系统，即根据用户名和为其指定的客户机地址的清单来核对用户名和客户机地址。

服务器若采用用户名与口令对用户进行认证，就必须维护合法用户的用户名与口令的数据库。以明文形式保存用户名，而用加密方式来保存口令。

WWW服务器一般以提供访问控制列表的方式来限制用户的文件访问权限。访问控制列表是文件和其他资源及有权访问这些文件和其他资源的用户名的清单或数据库。每个文件都有自己的访问控制列表。当客户机请求WWW服务器以便访问一个已设置好访问检查的文件时，WWW服务器即检查此资源的访问控制列表以确定此用户是否有权访问此文件。

（2）操作系统控制

操作系统为运行在其上的WWW服务器提供了安全子系统，UNIX和Windows操作系统是大多数WWW服务器的运行平台。

UNIX系统的资源访问控制是基于文件的，为了维护系统的安全性，系统中每一个文件都具有一定的访问权限，只有具有这种访问权限的用户才能访问该文件，否则系统将给出Permission或Denied的错误信息。有3类用户：用户本人、用户所在组的用户、其他用户。允许权：R—读，W—写，X—执行。允许权组：A—管理员（所有权利），V—属主，G—组，O—其他每个人。

Windows的NTFS文件系统是一种安全的文件系统，因为它支持文件访问控制，人们可以设置文件和目录的访问权限，控制谁可以使用这个文件，以及如何使用这个文件。5个预定义的许可为：拒绝访问、读取、更改、完全控制和选择性访问。

（3）为电子商务服务器配置防火墙

防火墙在内网和外网之间建立了一层保护，通常也是第一道保护。公司同互联网间的通信都要经过防火墙，要保护的网络和计算机放在防火墙内，其他网络则处在防火墙之外。防火墙相当于一个过滤设备，它允许特定的信息流入或流出被保护的网络。

2. 如何配置Web服务器的安全特性

（1）检查危及安全的漏洞

通常，如果IP地址设置不正确，就不能转换。一旦Web服务器获得IP地址和客户可能的域名，它就开始执行一系列验证手段。这里，有3个安全漏洞。

① 客户可能永远得不到要求的信息，因为服务器伪造了域名。客户可能无法获得授权访问的信息。

② 服务器可能向另一用户发送信息，因为客户伪造域名。

③ 误认闯入者是合法用户，服务器可能允许闯入者访问。

（2）加强服务器的安全的具体措施

① 认真配置服务器，使用它的访问和安全特性。

② 可将 Web 服务器当做无权的用户运行。

③ 检查驱动器和共享的权限，将系统设为只读状态。

④ 可将敏感文件放在基本系统中，再设二级系统，所有的敏感数据都不向互联网开放。

⑤ 充分考虑最糟糕的情况后，配置自己的系统。

⑥ 检查 HTTP 服务器使用的 Applet 脚本和客户交互作用的 CGI 脚本。防止外部用户执行内部指令。

⑦ 建议在 Windows NT 类服务器上运行 Web 服务器，这样会比较安全，尽管它不能提供像 UNIX 和 Sun 那样多的功能。

例如，IIS 7.5 服务器的安全配置规则如下。

① 匿名账户使用默认的“应用程序用户”，也就是对应的 IUSR。

② 应用程序池账户使用默认的 IIS AppPool\应用程序池名称。

③ 删除 everyone，users 在所有磁盘上的权限。

④ 删除 users 在 system32 上的所有权限（需要先修改所有者为 administrator）。

⑤ 在网站目录下给予 IUSR 读取权限。

⑥ 在网站目录下给予 IIS AppPool\应用程序池名称读取权限，如果程序中有特殊要求的权限，如写入文件等，则再对应的目录下给予相应的权限，如写入权限。

⑦ 在网站要求的上传目录给予 IIS AppPool\应用程序池名称写入权限，但是不给予执行权限。

⑧ 在 IIS 中取消上传目录的脚本执行权限。

3．如何排除站点中的安全漏洞

最基本的安全措施是排除站点中的安全漏洞，使其降到最少，通常表现为以下 4 种方式。

① 物理的漏洞由未授权人员访问引起，由于他们能浏览那些不被允许的地方。用户不仅能浏览 Web，而且可以改变浏览器的配置并取得站点信息，如 IP 地址、DNS 入口等。

② 软件漏洞是由“错误授权”的应用程序引起的。例如，脚本和 Applet，它会执行不应执行的功能。一条首要规则是：不要轻易相信脚本和 Applet。使用时，应确信能掌握它们的功能。

③ 不兼容问题漏洞是由不良系统集成引起的。一个硬件或软件运行时可能工作良好，一旦和其他设备集成后（如作为一个系统），就可能出现问题。这类问题很难确认，所以对每一个部件在集成进入系统之前，都必须进行测试。

④ 缺乏安全策略。如果用户用他们的电话号码作为口令，无论口令授权体制如何安全都没用。必须有一个包含所有安全必备（如覆盖阻止等）的安全策略。

4. 防止和追踪黑客闯入和内部滥用

为了防止和追踪黑客闯入或内部滥用，需要对 Web 站点上的出入情况进行监视控制。

（1）监控请求

① 服务器日常受访次数是多少？受访次数增加了吗？

② 用户是从哪里连接的？

③ 一周中的哪天最忙？一天中的何时最忙？

④ 服务器上哪类信息被访问最多？哪些页面最受欢迎？每个目录下有多少页面被访问？

⑤ 每个目录下有多少用户访问？访问站点的是哪些浏览器？与站点对话的是哪种操作系统？

⑥ 更多选择的是哪种提交方式？

（2）测算访问次数和访问者数目

以下两个指标直接影响安全保护，也会促进安全性的提高和改善。

① 确定站点访问次数。访问次数是一个原始数字，仅仅描述了站点上文件下载的平均数目。

② 确定站点访问者数目。将访问次数与主页文件联系在一起时，该数字接近于某个时期内访问者数目，但不是百分之百的准确。

（3）传输

Web 由传输协议、数据格式（HTML）及浏览器组成。使用协议、数据格式或浏览器，无须任何特别要求。

（4）传输更新

Web 站点的链接信息必须不停地更新、重建与改变，否则，将严重限制 Web 站点的服务质量。一般来说，Web 站点只允许单一种类的文本作为连接资源。

Apache 是一个非常优秀的 Web 服务器。Apache 的安装维护中需要注意以下问题。

① 检查文件和目录的权限是否恰当。

② httpd.conf、srm.conf 和 access.conf 文件的设置是否适当。

③ 使服务器日志文件能够记录尽可能详细的信息。

④ 对某些需要特别保护的目录使用密码保护（.htaccess）。

⑤ 对 CGI 脚本或者程序进行封装。

⑥ 如果 CGI 使用 Perl 编写，要详细检查其安全性。

⑦ 检查 SSI 命令。

⑧ 使用 TCP Wrappers 和 Tripwire。

1.3 电子商务安全问题

1. 电子商务活动的内容

从商务活动的角度看，电子商务活动整体上大致包括以下 3 个方面。

① 电子商务信息必须通过计算机网络进行传输。