CHAPTER 8

第 8 章 Web 站点规划设计、性能优化及安全性

学习要点
（1）了解 Web 站点分类。 （2）熟悉 Web 站点建设的流程。 （3）了解 Web 站点规划与设计的一般性原则。 （4）掌握 Web 站点性能优化和提高其安全性的技术措施。

Web 开发的目的就是建设一个 Web 站点应用系统。在 Web 站点建设之前必须对 Web 站点进行总体规划和设计，对 Web 站点主题、内容和风格等进行统一部署和规划，具体工作包括 Web 站点内容的组织、页面的目录结构、链接结构、页面组成、布局结构以及网页的各部分元素分布应该采用什么样的颜色，如何搭配等。Web 站点建设过程中还必须考虑 Web 站点的访问性能和安全性问题。本章主要介绍 Web 站点建设的总体规划过程，并在 Web 站点性能和安全性方面给出一些方法与原则，使读者对构建 Web 站点的整个过程有一个清晰和明确的了解。

8.1 Web 站点的分类及运行目的

8.1.1 Web 站点分类

Internet 上的 Web 站点数不胜数，与日俱增，对于 Web 站点的分类并没有固定的标准。一般来说 Web 站点可大致按以下的方式进行分类。

1．按 Web 站点的商业性质划分

Web 站点可分为商业性和非商业性 Web 站点。商业性 Web 站点是以商品交易或提供服务等为目的的 Web 站点。例如淘宝网(http://www.taobao.com)、京东商城网（http://www.360buy.com/）等都属于商业性 Web 站点。

2．按 Web 站点服务对象的区域划分

Web 站点可以划分为区域性 Web 站点和非区域性 Web 站点。区域性 Web 站点就是

Web 站点主题围绕特定地区服务的 Web 站点。例如，重庆信息网（http://www.cqxxw.net/）就是一个以重庆地区为特定服务对象的区域性 Web 站点。

3．按 Web 站点的所有权划分

按 Web 站点的所有权进行划分，Web 站点可划分为政府性 Web 站点、学校 Web 站点、企事业 Web 站点、组织性 Web 站点、个人 Web 站点等。

例如，重庆市政府公众信息网（http://www.cq.gov.cn/）是一个政府性 Web 站点。重庆大学网（http://www.cqu.edu.cn）是一个学校 Web 站点。重庆长安网（http://www.changan.com.cn/）是一个企业 Web 站点。中国网（http://www.china.org.cn）是一个组织性的 Web 站点。

4．按组成网页的形式划分

按组成网页形式的不同可将 Web 站点分成文字型 Web 站点和图片型 Web 站点。前者主要是由文字构成的，例如新浪网（http://www.sina.com），而后者则以图片为主，如“可口可乐中国”Web 站点（http://www.coca-cola.com.cn）。

5. 按 Web 站点使用范围划分

按 Web 站点使用范围进行划分可划分为大众型、企业型和局部型 Web 站点。大众型 Web 站点面向所有互联网上的用户，例如 Google、搜狐、QQ 等。企业型 Web 站点面向企业用户，企业的业务处理在互联网上都通过该站点来实现。局部型 Web 站点是指位于企业内联网上的 Web 站点。

8.1.2　Web 站点的运行目的

Web 站点的运行目的主要包括信息服务、教育和娱乐、办公和信息管理、电子商务等。

1. 信息服务

许多站点建设的目的是提供信息服务，分为无偿和有偿信息服务。例如学校、政府、企业形象宣传、企业商品信息的发布等都是免费的，而很多网站大都提供有偿信息服务。

2．教育和娱乐

教育机构、培训机构等构建 Web 站点的目的是提供网上教育服务，例如网上学校、远程教学、网上培训……另外大量游戏、音乐、视频网站等用于公众娱乐。

3．办公和信息管理

站点建设的目的主要是为了提供办公自动化或者进行企业的信息化管理等。

4．电子商务

电子商务模式主要有：B2B（Business to Business）、B2C（Business to Customer）、C2C（Customer to Customer）、BforC（Business For Customer）等。

B2B 指的是商家（泛指企业）对商家的电子商务，即企业与企业之间通过互联网进行产品、服务及信息的交换。通俗的说法是指进行电子商务交易的供需双方都是商家（或企业、公司），它们使用了 Internet 的技术或各种商务网络平台，完成商务交易的过程。这些过程包括：发布供求信息；订货及确认订货；支付过程及票据的签发、传送和接收；确定配送方案并监控配送过程等。

B2C 即商家对消费者，也就是通常说的商业零售，直接面向消费者销售产品和服务。最具有代表性的 B2C 电子商务模式就是网上零售网站，例如中文网上书店当当网、美国的

亚马逊网上商店等都是 B2C 电子商务网站。

C2C 即个体用户对个体用户，或者说是个体用户之间的电子商务，即个体用户与个体用户之间通过互联网进行产品、服务及信息的交换。例如 eBay、易趣、淘宝、拍拍网等。

BforC 是指中小企业和个人消费者的任何零星采购都将享受到“团购”价格，使消费者喜欢的团购不再受时间、地点、型号的限制，真正实现“随时随地的团购”。

8.2 Web 站点的目录结构和链接结构

8.2.1 Web 站点的目录结构

Web 站点的目录是指建立 Web 站点时创建的目录。浏览者并不关心目录结构的好坏，但它对站点的维护、未来内容的扩充和移植都会有重要的作用。下面是建立 Web 站点目录结构的一些建议。

（1）不要将网站内容全部放在一个目录中，按菜单栏目内容建立子目录。

将网站内容全部放在一个目录中会造成文件管理混乱，很难维护。管理员常常会搞不清哪些文件需要编辑和更新，哪些无用的文件可以删除，哪些是相关联的文件。另外服务器一般都会为网站建立一个文件索引，如果将所有文件都放在一个目录中，在重新建立索引时影响服务器性能。

建议按主菜单栏目建立子目录。例如企业站点可以按公司简介、产品介绍、价格、在线订单、反馈联系等内容建立相应子目录。而一些相关性强、不需要经常更新的栏目可以合并放在一个统一目录下。对于图片可以在根目录下建立一个存放图片的子目录，用于存放各个栏目共用的图片，再在各个栏目下设立图片子目录，存放各个栏目内所需要的图片。

（2）目录的层次不要太深，尽量用英文命名目录和文件名。

一般来说，Web 站点的目录层次不要超过 3 层，这样便于维护管理。目录路径过深，跳转的 URL 地址就会变长，会增加页面的链接复杂性。使用中文命名目录和文件名可能对网址的正确显示造成困难，应尽量使用英文命名目录和文件名，而且应尽量使用英文意义明确的目录名和文件名，便于维护和管理。要注意一般目录名和文件名可达 255 个字符，但请不要使用过长的名字（请读者思考为什么）。

8.2.2 Web 站点的链接结构

Web 站点的链接结构是指页面之间相互链接的拓扑结构，它建立在目录结构基础之上，而且可以跨越目录。Web 站点的链接结构有三种基本方式：

（1）树状链接结构。这种结构类似于目录结构。首页链接指向一级页面，一级页面链接指向二级页面。浏览这样的链接结构时，用户可以一级级进入，一级级退出。这种结构的优点是条理清晰，访问者可以明确地知道自己在什么位置，不会“迷路”。它的缺点是浏览效率低。用户从一个栏目下的子页面到另一个栏目下的子页面，必须绕经首页。

（2）星状链接结构。这种结构类似于 Web 服务器之间的链接，结构中的每个页面相互之间都建立了链接。这种链接结构的优点是浏览方便，访问者可以随时到达自己想要的页面。缺点是链接太多，容易使浏览者迷路，搞不清自己在什么位置。

（3）混合结构。在实际的 Web 站点设计中，总是将以上两种结构混合起来使用，希望浏览者既可以方便快速地到达自己需要的页面，又可以清晰地知道自己的位置。比较好的解决方法是：首页和一级页面之间用星形链接结构，一级和二级、二级和三级页面之间均采用树型结构。这样既提高了浏览效率，又提高了站点结构的清晰程度，如图 8-1 所示。

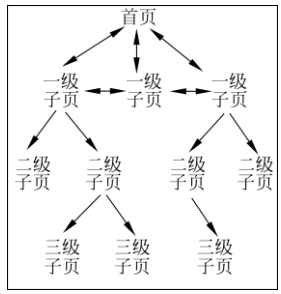

图 8-1　混合链接结构

8.3　Web 站点的主题、名称和 Logo 标志

建设一个网站首先要确定网站所属类别下的主题。主题是 Web 站点的灵魂，一个好的 Web 站点首先需要好主题。Web 站点若没有准确的定位，内容太过丰富庞杂，再好的色彩搭配和特效，也会缺少吸引力。

一旦确定站点主题，就应该围绕主题给 Web 站点起一个名字即 Web 站点名称。Web 站点名称对 Web 站点的形象和宣传推广有很大影响。例如“电脑学习室”和“电脑之家”显然是后者简练；“儿童天地”和“中国幼儿园”显然是后者大气。Web 站点的名称选择一般来说应合情、合理、合法，不能用色情的、迷信的、反动的、危害社会安全的名词。名称能体现 Web 站点的内涵，给浏览者更多的新意和空间想象力。例如黑客基地、久听音乐和图书时空等。Web 站点的名称尽量不要使用中英文混合的名称，也不能太长，要简单易记。

站点标志作用类似于商标，它是 Web 站点特色和内涵的集中体现。Web 站点强大的整体实力、优质的产品和服务都被涵盖于标志中。通过不断地刺激和反复地刻画，标志将深深地留在网民心中，从而让网民一看见 Logo 就能联想起相应的 Web 站点。具有长远眼光的企业十分重视 Logo 设计，在 Web 站点建设初期，好的设计无疑是日后无形资产积累的重要载体。最常用和最简单的方式是将自己 Web 站点的名称作为标志，将不同的字体、字母的变形等组合起来可以很容易地制作好自己的标志，如搜索引擎 Google 的标志，就很有动感特色。

8.4　Web 站点规划的内容

Web 站点规划是指在 Web 站点建设前对市场进行分析、确定 Web 站点的目的和功能，并根据需要对 Web 站点建设中的技术、内容、费用、测试、维护等做出规划。在建立 Web 站点前应明确建设 Web 站点的目的、确定 Web 站点的功能、确定 Web 站点规模、投入费用，并进行必要的市场分析等。只有详细地规划，才能避免在 Web 站点建设中出现问题，使 Web 站点建设能顺利进行。

Web 站点规划的内容包括以下几个方面。

1．建设 Web 站点前的市场分析

（1）相关行业的市场是怎样的？市场有什么样的特点？是否能够在互联网上开展公司业务？

（2）市场主要竞争者分析，包括竞争对手 Web 站点情况及其功能作用。

（3）公司自身条件分析，包括公司概况、市场优势、可以利用 Web 站点提升哪些竞争力、建设 Web 站点的能力（费用、技术、人力等）。

2．建设 Web 站点的目的及功能定位

（1）为什么要建立 Web 站点？是为了宣传产品，进行电子商务，还是建立行业性 Web 站点?是企业的需要还是市场开拓的延伸?

（2）整合公司资源，确定 Web 站点功能。根据公司的需要和计划，确定 Web 站点的功能，如产品宣传、网上营销、客户服务、电子商务等。

（3）根据 Web 站点功能，确定 Web 站点应达到的目的。

（4）企业内部网的建设情况和 Web 站点的可扩展性。

3．Web 站点技术解决方案

根据 Web 站点的功能确定 Web 站点技术解决方案。主要包括：

（1）服务器选择。采用自建服务器，还是租用虚拟主机。

（2）操作系统选择。用 UNIX、Linux 还是 Windows。

（3）解决方案选择。是自己开发还是采用现有的方案。具体描述其实施方案。

（4）分析相应的投入成本、运行费用、稳定性和安全性等。

4．Web 站点内容规划

（1）根据 Web 站点的目标和功能规划 Web 站点内容。一般企业 Web 站点应包括公司简介、产品介绍、服务内容、价格信息、联系方式、网上订单等基本内容。

（2）电子商务类 Web 站点要提供会员注册、详细的商品服务信息、信息搜索查询、订单确认、付款、个人信息保密措施、相关帮助等。

（3）如果 Web 站点栏目比较多，应考虑采用专人负责相关栏目。Web 站点内容是吸引浏览者最重要的因素，无内容或不实用的信息不会吸引匆匆浏览的访客。如果事先对人们希望阅读的信息进行调查，并在 Web 站点发布后调查人们对 Web 站点内容的满意度，便可以及时调整 Web 站点内容。

5．网页设计

（1）网页美术设计一般要与企业整体形象一致，要符合规范。要注意网页色彩、图片的应用及版面规划，以保持网页的整体一致性。

（2）在新技术的采用上要考虑主要目标访问群体的分布地域、年龄阶层、网络速度、阅读习惯等。

（3）制定网页改版计划，如半年到一年时间进行较大规模改版等。

6．Web 站点测试

规划在完成 Web 站点后将要进行哪些测试和如何进行测试，测试的指标是什么等。

7．Web 站点发布与推广

Web 站点测试后将采用什么方法进行发布，规划 Web 站点的推广策略。

8．Web 站点维护

（1）服务器及相关软硬件的维护。对可能出现的问题进行评估，制定响应时间。

（2）数据库维护。Web 站点维护的一项重要内容就是数据库维护。

（3）内容的更新、调整等。

（4）制定相关 Web 站点维护的规定，将 Web 站点的维护制度化、规范化。

9．Web 站点建设日程表

规划各项任务的开始及完成时间，负责人等。

10．费用明细

各项事宜所需费用清单。

以上为 Web 站点规划设计报告书中应该体现的主要内容，根据不同的需求和建站目的，内容也会有所增加或减少。在建设 Web 站点之初一定要进行精心规划，才能达到预期建站目的。

8.5　设计 Web 站点的一般性原则

下面是 Web 站点设计中的一般性原则。

1．以客户为中心进行 Web 站点设计

站点是展现企业形象、介绍产品和服务、体现企业发展战略的重要途径，因此必须明确设计站点的目标和用户需求，从而做出切实可行的设计方案。要根据客户的需求、市场的状况、企业自身的情况等进行综合分析和设计。在设计规划之初要考虑如下问题：建设 Web 站点的目的是什么？为谁提供服务和产品?企业能提供什么样的产品和服务？Web 站点的目标消费者和受众的特点是什么？企业产品和服务适合什么样的表现方式（风格）?

2．总体设计方案主题鲜明

在目标明确的基础上，对 Web 站点的整体风格和特色做出定位，对 Web 站点的组织结构进行规划。好的 Web 站点应该主题鲜明、要点明确，要充分利用各种技术手段表现 Web 站点的个性和情趣，体现 Web 站点的特色。

3．网页形式与内容统一

运用对比与调和、对称与平衡、节奏与韵律以及留白等手段，利用空间、文字、图形之间的相互关系来达到整体的均衡以及和谐的美感。如对称原则的运用在页面设计时有可能会使页面显得呆板，但如果加入一些富有动感的文字、图案，或采用夸张的手法来表现内容往往会达到更好的效果。点、线、面是视觉语言中的基本元素，要使用点、线、面的互相穿插、互相衬托、互相补充才能构成最佳的页面效果。

4．Web 站点的结构

在设计 Web 站点结构时，应遵循结构清晰、导向清楚、使用方便的原则。应使用一些醒目的标题或文字来突出产品与服务，在导航设计中使用超文本链接或图片链接，并且页面之间的链接关系要一目了然。

5．访问速度

应想方设法提高 Web 站点的访问速度，例如通过网页减肥、Ajax 技术等来加快访问速度。绝大多数浏览者不会进入需要等待 1min 才能进入的 Web 站点。设计 Web 站点应尽

量避免使用过多的图片及尺寸过大的图片。设计 Web 站点时最好将主要页面的容量控制在 50KB 以内，平均 30KB 左右，以确保普通浏览者等待页面的时间不超过 10s。

6．充分利用多媒体技术

为了吸引浏览者的注意力，页面内容应采用动画、Flash 等形式来表现。但要注意由于网络带宽的限制，在使用多媒体形式来表现网页内容时应考虑客户端的传输速度。

7．Web 站点信息的动态发布

站点信息的不断更新，会让浏览者了解企业的最新发展动态和网上服务等，同时也会帮助企业建立良好的形象。应在后台建立信息的动态发布机制及时更新企业站点内容。

8．提供和用户相互沟通的渠道

在企业的 Web 站点上，应建立和用户的沟通渠道，例如建立留言板和在线 E-mail 系统、短消息等。

总之，合理的 Web 站点框架结构、优化的网页布局、友善的访问浏览方式、精美的视觉效果、适宜的创意设计是设计 Web 站点应遵循的基本原则。

8.6 建设 Web 站点的一般步骤

建立 Web 站点和做其他任何项目一样，Web 站点的规划是成功的关键。建立 Web 站点首先要明确建立 Web 站点的目的是什么，并对目标进行分析，从市场观念风险、技术风险、执行风险、组织风险、政策风险等方面综合考虑，然后最终确定 Web 站点建立的目标和实施策略，接着进行费用预算和制定时间表。

在确定 Web 站点目标后，需要申请域名，安装 Web 服务器、邮件服务器、数据库服务器等，并确定 Web 站点接入 Internet 的方法，然后通过 Web 开发工具进行 Web 站点设计和开发，最后进行 Web 站点调试，调试成功后最终正式开通 Web 站点。

1．Web 站点准备阶段

需要建立一个 Web 站点时，首先要做的事情就是冷静下来、认真思考和计划，进行可行性分析，根据建立 Web 站点的目标，规划出 Web 站点的大致结构。考虑采用哪一种操作系统，因为不同的操作系统将采用不同的 Web 服务器、邮件服务器、数据库服务器。采用数据库系统建立的 Web 站点可以极大地提升 Web 站点的功能，因此进行数据库的初步规划是必要的，还必须考虑开发一个 Web 站点并维持 Web 站点运行的费用问题。准备工作基本确定后，下一步就是域名注册。

2．域名注册

域名注册实际上就是申请 Web 站点的一个名称，以方便人们来访问 Web 站点。域名是在 Internet 中用于解决地址对应问题的一种方法，代表着一个 IP 地址。域名存放在一个数据库中，有一些服务器专门负责域名与 IP 地址的解析工作，该服务器称为域名服务器 DNS（Domain Name Server）。域名具有唯一性，已被企业誉为“企业的网上商标”。域名区分为国际域名和国内域名，例如 sina.com 为国际域名，而 sina.com.cn 为国内域名。域名中.com 表示工、商、金融企业；.edu 表示教育机构；.gov 表示政府部门；.net 表示网络服务部门；.ac 表示科研机构。国内域名中.cn 表示中国，其他如.hk 表示中国香港特别行政区；.us 表示美国，等等。申请国际域名还是申请国内域名，应该根据 Web 站点的服务范

围来选择，如果 Web 站点服务范围仅限于国内，则可以考虑申请一个国内的域名，如建立的 Web 站点面向全球提供信息服务，可以申请一个国际域名。当然不管你申请国际域名还是国内域名，都一样可以被 Internet 上的任何用户访问。域名相当于网上商标，因此最好国内和国际域名一同注册。注册一个域名后，注册机构按年收取一定费用。

注册域名时应首先确定一个域名，域名应简短、切题、通俗。国际域名是否已经被注册可通过 http://www.interNIC.org（国际互联网络信息中心 interNIC）或者 http://www.networksolutions.com 站点进行检查；国内域名是否已经被注册可通过 http://www.cnnic.com.cn（中国互联网络信息中心 CNNIC）站点进行检查。注册国际域名没有条件限制，单位和个人均可以申请。注册国内域名则必须具备法人资格。申请人需将申请表加盖公章，连同单位营业执照副本（或政府机构条码证书复印件）提交给相关注册服务商才能申请注册。国际域名与国内域名在功能上没有任何区别，都是互联网上唯一的企业标识，只是在最终管理机构上有所区别。注册国际域名由国际域名管理机构 interNIC 负责受理，手续非常简便，只需上网到相关 Web 站点，填写注册表后提交，30 天内支付注册费后即可开通。国内域名注册的权威机构是 CNNIC。网上有很多 Web 站点（例如中国万网）提供域名注册服务，可以通过该 Web 站点在线注册国内域名和国际域名，它们的注册费用各不相同，有的还是免费的。

3．Web 站点的需求分析和总体设计

在建设一个网站之前，不必一开始就忙着准备素材，首先要完成站点的需求分析和总体设计。需求分析是网站设计的重要环节。需求分析工作做得越细，对网站的建设成功就越有帮助，用户对网站设计方案的认可度就越高，就越能达到用户的最大满意度。在需求分析的基础上进行总体设计和数据库设计。在此过程中确定站点建设所需要的软件和硬件配置、连接因特网的方式、运行和维护费用等。

4．确定 Web 站点的组织与风格

在上述工作基础上，确定 Web 站点的主页版面，色彩搭配等，勾画出整个 Web 站点系统的所有全貌，包括每个页面的版式布局、链接关系、注意事项等。Web 站点的结构层次不能太深，应遵从“三次单击”原则，即 Web 站点的任何信息都应该在最多三次单击后找到。另外也要注意结构层次不能太浅，什么东西都放在一个页面上，给人以 Web 站点组织混乱、设计者毫无经验的印象。应该确定一种方法使得网页内容可以在 Internet Explorer 和 Netscape 两种主流浏览器中都能被正常显示，一般通过在页面脚本程序中针对不同浏览器进行控制来实现。

Web 站点的组织与风格是至关重要的。有些 Web 站点充满了各种“酷”的特效和五彩缤纷的图片，却无实际内容；有些 Web 站点只重视提供信息，但界面却显得呆板、乏味，等等，因此必须精心安排和组织页面。一个成功的网页应包含 Web 站点名称、Web 站点徽标、网页标题、网页内容、指向主页的链接、指向其他网页的链接、版权陈述、Web 站点的 E-mail 地址和其他联系方法等等基本要素。

一个网页的长度一般应控制在 2 页到 3 页的篇幅内，太短则无法容纳足够的信息，太长则使网页下载的时间变长，可能会使人们失去耐心而转向其他 Web 站点，也会使人们因为长长的网页拖动滚动条而搞得晕头转向。

在进行网页的版面设计时应注意页面的简洁性和高效性，让人们易于找到所关心的信

息，不要让精美的动画和花哨的图片喧宾夺主。Web 站点应确定一个主色调和一个统一的字体风格、图素风格等。所有的网页都要采用这个主色调和风格。颜色搭配要协调，过于繁多和凌乱的颜色会使人们感到无所适从。页面布局采用框架结构还是采用表格方式应根据实际情况确定。框架结构是将整个屏幕分成若干个小区域，每一区域可以显示不同的网页，单击某一区域上的超链接除了可以在本区域显示另一页面外，还可在另外一个区域显示对应此超链接的页面文档，而其他区域的页面不必重新下载，唯一不便之处是对于不同的浏览器可能显示的结果不会完全一致。目前很多 Web 站点采用表格方式来布局页面，虽然每次访问均须下载整个页面，但主要解决了浏览器的兼容问题。页面中采用导航条可以使人们在浏览页面时不会迷失方向。导航条实际上就是一组超链接，它告诉人们目前所在的位置，可以使人们既快又容易地转向 Web 站点的其他主要页面。

在设计 Web 站点时还应注意以下几点：抓住能传达主要信息的字眼作为超链接；图像或图形的超链接，应配以文字说明，以便人们关闭图形显示时可以看文字说明；不要在短小的网页中提供太多的超链接；注意超链接文本的颜色应该与普通文本的颜色有所区别。通常采用层叠样式单（CSS）来保持页面的字体、字体颜色、背景、边框、文本属性等风格的一致。

5．Web 站点开发和运行环境的确定

根据站点运行的实际情况确定 Web 站点的运行环境。Web 站点运行的操作系统目前主流有两种：Windows 系统和 Linux 系统。究竟选用哪一种操作系统都无关紧要，一般认为选用 Linux 系统在网络安全性方面要比 Windows 系统要好，但这并不意味着 Linux 不存在安全性问题。在 Windows 下对于一般性 Web 站点比较理想的运行环境是 Windows Server 2008 操作系统 + IIS 7.0 Web 服务器 + Microsoft SQL Server 2005/2008 数据库服务器。Java EE 和.NET 开发平台各领风骚，一般认为用 Java 平台开发的站点其安全性和运行效率要优于.NET 平台开发的站点。但 Java 平台提倡开源，工具的多样性和复杂性造成对开发者的要求很高，增加了开发难度和系统的维护成本，而.NET 则易于学习和使用，站点易于实现，系统维护成本低。

6．Web 站点的开发

Web 站点的开发涉及到项目负责人、设计人员、程序员、网页制作人员和美工等。其中项目负责人负责站点内容的总体设计、进度和人员安排等；设计人员负责站点页面布局和整个站点程序的设计、数据库设计等工作；程序员主要负责服务器端程序开发等；网页制作人员负责开发网页工作等；美工人员则负责制作动画和图片，并嵌入到网页中去。

通过 Dreamweaver、VS 2010 等工具来建设 Web 站点可大大提高工作效率。目前在 Windows 系统下建立 Web 站点的最好工具还是 VS 2010，它是一个集成的开发平台。但 VS 2010 中的页面生成工具功能相对较弱，因此结合 Dreamweaver 强大的页面文档生成器，进行 Web 站点的开发是相当方便的。例如在 Dreamweaver 中，提供了大量的自动生成页面脚本程序的功能，利用它将生成的脚本程序粘贴到 VS 2010 中可节约很多时间。建设 Web 站点过程中掌握 VBscript 或 JavaScript 脚本语言的使用是必需的，这些脚本语言又区分为客户端运行的脚本和服务器端运行的脚本。只有灵活使用这些脚本语言，才可以开发出活泼、动态的交互式动态 HTML 页面。

7．Web 站点的测试

在 Web 站点开发过程中，网站测试是保证整体项目质量的重要一环。当把各个网页整合成网站后，要对整个网站进行测试。看其是否能够正常运行，并将其中的运行错误加以修改。主要测试内容有：功能测试和性能测试、安全性测试、稳定性测试、浏览器兼容性测试、链接测试等。可通过一些专业工具检查链接错误，找出网页制作中存在的各种问题。

8．将 Web 站点接入 Internet，并做好网站推广

Web 站点开发成功后，需要放到 Internet 网上作为一个网络结点被网上用户访问。根据情况，选择虚拟主机方式、服务器租用或托管方式、铺设专线方式来接通 Internet，供人们访问。

虚拟主机是使用特殊的软硬件技术，把一台计算机主机分成多台“虚拟”的主机，每一台虚拟主机都具有独立的域名和 IP 地址（或共享的 IP 地址）且有完整的 Internet 服务器（包括 WWW、FTP、E-mail 等服务）功能。在这种模式下，同一台硬件、同一个操作系统之上，运行着为多个用户启动的不同的服务器程序，且互不干扰；而各个用户又拥有自己的系统资源（IP 地址、文件存储空间、内存、CPU 时间等）。虚拟主机之间完全独立，并可由用户自行管理。在外界看来，每一台虚拟主机和一台独立的主机完全一样。使用网络公司的“虚拟主机”服务，就是在别人的主机上租用一定的网站空间以架设自己的网站。网络公司不仅可以为客户提供存放网页的空间,同时也可以开设数目不定的电子邮件账号。使用虚拟主机可以节省购买相关软硬件设施的费用，而且公司也无须招聘或培训更多的专业人员，因而其成本很低，但虚拟主机只适合于一些小型的、结构较简单的网站。

服务器租用或托管方式就是在租来的或自备的服务器上安装和配置好 Web 站点，然后安放到一些专门的网络服务机构，每年支付一定数额的费用，通过远程登录方式进行站点维护。这种方式适合于较大型的网站。目前很多网站都是采用这种方式。

专线上网方式就是将站点服务器安放在企业内部，通过专线连接于互联网。这种方式成本最高。站点运行费用中线路租用费用是一笔很大的费用。

对于商业 Web 站点，正式开通后，并不代表就大功告成了，必须实施推广活动。如何宣传自己的 Web 站点就成为 Web 站点能否发挥其作用的关键所在。站点推广是指通过各种有效的手段提高 Web 站点知名度，提升 Web 站点访问量。推广活动有长期和短期的；有无偿的和有偿的；有费用高的和费用低的，当然效果也有所不同。比较简单的是通过群发邮件、在各大论坛注册后讨论、让搜索引擎帮忙等方式来推广，在这方面使用一些适当的技巧,可以得到百倍于投入的收益。

9．Web 站点的运行安全和维护管理

涉及到 Web 站点的安全性方面的问题比较多，主要包括：身份窃取、数据窃取、假冒、非授权存取、错误路由、否认、拒绝服务，等等。在站点服务器上要保证操作系统的漏洞及时得到修复，精心配置 Web 服务器、邮件服务器、数据库服务器的各项参数设置。本章后面将详细讨论 Web 站点的安全性。Web 站点的维护和管理包括服务器的维护、站点程序的维护、内容的更新和信息的发布等。主要工作包括要对存在的问题进行修改、对 Web 站点内容进行更新或修改、及时清除一些垃圾页面或图片、对数据库进行备份等。

8.7 Web 站点性能优化

Web 用户总是希望在当前网络带宽情况下，所访问的网站响应速度足够快，能够很快找到所关心的信息。对 Web 站点提供者来说，要求 Web 站点能够容纳更多访问者的同时，保持用户的高速访问性能。当一个站点访问用户过多时，服务器会超载，站点速度也会随之降低。增加服务器和扩充内存并运用负载均衡或群集方案，可增加 Web 站点访问量，大大提高站点的性能，但硬件和维护成本也会大大增加，且可能 Web 用户可以获得较快的访问速度，但预期的访问量却达不到，造成资源浪费。因此应首先考虑通过优化 Web 服务器配置、改善 Web 应用程序的性能来提高整个站点的访问性能。

8.7.1 优化 Web 服务器硬、软件配置

使用快速的磁盘和好的网络存取机制，能明显改进 Web 站点访问速度。可以运用特定网卡（如 Akamba 公司的 Velobahn）来改进服务器的速度，或是采用相关技术优化网络接口卡的性能。这类网卡可减轻 Web 服务器 CPU 的负荷，使其从繁琐的网络协议处理中解脱出来，而集中于页面处理和服务提供。可以为 Web 服务器增加反向缓冲代理，使服务器能够顺利实现已创建页面的传输，同时在创建动态页面过程中减轻服务器负荷。可以通过对数据库服务器和 Web 服务器的配置在缓冲、压缩、带宽限制、进程限制等方面提高 Web 站点的性能。

8.7.2 改善 Web 应用程序的性能

Web 站点的性能除了和网络状况、硬件配置相关外，不容忽视的是和 Web 开发人员的开发水平有关。为提高站点的访问性能，Web 开发人员应注意以下方面的问题（以开发 ASP.NET 应用程序为例）。

1．帮页面“减肥”

我们在浏览网页时实际上是将 Web 站点的网页内容下载到本地硬盘，再用浏览器解释查看的。下载网页的快慢在显示速度上占了很大比重，所以网页本身所占的空间越小，那么浏览速度就会越快。这就要求在做网页的时候遵循一切从简的原则，如：不要使用太大的 Flash 动画、图片等资源；设法减少 GIF 文件对颜色的使用，并调整 JPEG 文件大小；删除页面中无用的符号，例如空格和不必要的注解；等等。目前有很多网页减肥器软件可以帮助减少网页的大小。

2．尽量使用静态 HTML 页面

ASP/ASP.NET、PHP、JSP 等程序实现了网页信息的动态交互，运行起来的确非常方便，因为它们的数据交互性好，能很方便地存取、更改数据库的内容，使 Web 站点动起来。但这类程序必须先由服务器执行处理后，生成 HTML 页面，然后再送往客户端浏览，这就不得不耗费一定的服务器资源。如果在 Web 站点上过多地使用这类程序，网页显示速度肯定会慢，所以应尽量使用静态的 HTML 页面。

3．切忌将整个页面内容塞到一个 Table 中

网页设计中，有些开发者为追求页面的统一对齐，将整个页面的内容都塞进了一个

Table 里，然后再由单元格 td 来划分各个块的布局，这种 Web 站点的显示速度是绝对慢的。因为 Table 要等里面所有的内容都加载完毕后才显示出来的，如果某些内容无法访问，就会拖延整个页面的访问速度。正确的做法是将内容分割到几个具有相同格局的 Table 中去，不要全都塞到一个 Table 里。

4. 将 ASP/ASP.NET、JSP、PHP 等文件的访问改为 js 文件引用

经常会遇到这样的问题：在站点的首页上需要显示数据库中存放的最新的几条新闻信息标题，以便人们点击新闻标题查看，于是开发人员就将首页变成动态服务器页面，在其中加入 ASP/ASP.NET、JSP、PHP 程序用以连接数据库、访问数据库以获取新闻标题。这样做从功能上说没有任何问题，问题是每一个访问网站的人都要让 Web 服务器连接数据库获取数据，当用户数较多的情况下，Web 站点的响应速度会很慢。数据库中的新闻信息的变更一般来说会通过后台新闻发布系统来更新，如果我们在后台每发布一个新闻的时候，在动态服务器页面中，自动生成一个 js 文件，将新闻标题以超链接的方式用 JavaScript 语言写好，例如：

```
//mynews.js 文件:
document.writeln("<A href='getnews.aspx?newid=10101'>新闻标题 1</A>");
document.writeln("<A href='getnews.aspx?newid=10102'>新闻标题 2</A>");
document.writeln("<A href='getnews.aspx?newid=10103'>新闻标题 3</A>");
document.close();
```

然后在首页放置新闻标题的地方通过 < SCRIPT src="mynews.js 文件">< /SCRIPT>这样的代码来引用该 js 文件，这样就可以将首页变成一个静态 HTML 页面，而不是动态服务器页面，这样就会大大提高首页的访问速度。

5．使用 iframe 嵌套另一页面

如果你要在 Web 站点上插入一些广告代码，又不想让这些广告影响 Web 站点的速度的话，那么，使用 iframe 最合适不过了。方法是将这些广告代码放到一个独立的页面去，然后在首页用如下的代码将该页面嵌入即可，这样就不会因为广告页面的延迟而拖了整个首页的显示，代码如下：

```
＜iframe align="center" width="780" height="30" name="all" scrolling="no"
marginWidth=0
frameborder="0" src="页面 URL">＜/iframe＞
```

6．站点计数器的放置位置

应将站点访问计数器放到页面代码的最下方，防止由于某种原因所引起的服务器超时延迟，导致页面很长时间才能访问。

7．数据库的连接和关闭

访问数据库资源需要创建连接、打开连接和关闭连接几个操作。这些过程需要多次与数据库交换信息以通过身份验证，比较耗费服务器资源。ASP.NET 中提供了连接池（Connection Pool）改善打开和关闭数据库对性能的影响。系统将用户的数据库连接放在连接池中，需要时取出，关闭时收回连接，等待下一次的连接请求。连接池的大小是有限的，如果在连接池达到最大限度后仍要求创建连接，必然大大影响性能。因此，在建立数据库连接后只

有在真正需要操作时才打开连接，使用完毕后马上关闭，从而尽量减少数据库连接打开的时间，避免出现超出连接限制的情况。

8．尽量使用存储过程

存储过程是存储在服务器上的一组预编译的 SQL 语句，类似于 DOS 系统中的批处理文件。存储过程具有对数据库立即访问的功能，信息处理极为迅速。使用存储过程可以避免对命令的多次编译，在执行一次后其执行规划就驻留在高速缓存中，以后需要时只需直接调用缓存中的二进制代码即可。另外存储过程在服务器端运行，独立于 ASP.NET 程序，便于修改，最重要的是它可以减少数据库操作语句在网络中的传输。

9．优化查询语句

ASP.NET 中 ADO 连接消耗的资源相当大，SQL 语句运行的时间越长，占用系统资源的时间也越长。因此，尽量使用优化过的 SQL 语句以减少执行时间。比如不在查询语句中包含子查询语句、充分利用索引等。

10．ASP.NET 中的编程注意事项

在 ASP.NET 编程中注意如下问题，可以提高 Web 站点的访问性能。

（1）选择适合的数据查看机制。根据你选择在 Web 窗体页显示数据的方式，在便利和性能之间常常存在着重要的权衡。例如，Gridview Web 控件可能是一种显示数据的方便快捷的方法，但就性能而言它的开销常常是最大的。Repeater Web 控件是便利和性能的折衷，它高效、可自定义且可编程。

（2）采用 Server.Transfer 重定向页面。在页面中使用该方法可避免不必要的客户端重定向。

（3）在部署 Web 站点时，不要启用调试模式。否则应用程序的性能可能会受到非常大的影响。不要禁用 Web 窗体页的缓冲，否则会导致大量的性能开销。

（4）将 SqlDataReader 类用于快速只进数据游标。SqlDataReader 类提供了一种读取从 SQL Server 数据库检索的只进数据流的方法。它提供比 DataSet 类更高的性能。

（5）字符串操作性能优化。使用值类型的 ToString 方法可以避免装箱操作，从而提高应用程序性能。使用“+”号连接字符串时由于涉及到不同的数据类型，数字需要通过装箱操作转化为引用类型才可以添加到字符串中，但装箱操作对性能影响较大。在处理字符串时，最好使用 StringBuilder 类，其.NET 命名空间是 System.Text。该类并非创建新的对象，而是通过 Append、Remove、Insert 等方法直接对字符串进行操作，通过 ToString 方法返回操作结果。

```
int num;
System.Text.StringBuilder str = new System.Text.StringBuilder(); //创建字符串
str.Append(num.ToString()); //添加数值 num
Response.Write(str.ToString); //显示操作结果
```

（6）应考虑编译运行 Web 应用程序。应尽量避免更改应用程序的\bin 目录中的程序集。更改页面会导致重新分析和编译该页，而替换\bin 目录中的程序集则会导致完全重新批编译该目录。在包含许多页面的大规模站点上，更好的办法可能是根据计划替换页面或程序

集的频繁程度来设计不同的目录结构。不常更改的页面可以存储在同一目录中并在特定的时间进行预批编译。经常更改的页面应在它们自己的目录中以便快速编译。

（7）不要依赖代码中的异常。异常大大地降低性能，所以不应将它们用作控制正常程序流程的方式。如果有可能检测到代码中可能导致异常的状态，请执行这种操作。不要在处理该状态之前捕获异常本身。请比较下面的代码，两者产生相同的结果。

```
try
{  result = 100 / num;  }
catch (Exception e)
{ result = 0;  }
// change to this:
if (num != 0)  result = 100 / num;
else  result = 0;
```

（8）只在必要时保存服务器控件视图状态。自动视图状态管理是服务器控件的功能，该功能使服务器控件可以在往返过程上重新填充它们的属性值（你不需要编写任何代码）。但是，因为服务器控件的视图状态在隐藏的窗体字段中往返于服务器，所以该功能确实会对性能产生影响。你应该知道在哪些情况下视图状态会有所帮助，在哪些情况下它影响页的性能。例如，如果你将服务器控件绑定到每个往返过程上的数据，则将用从数据绑定操作获得的新值替换保存的视图状态。在这种情况下，禁用视图状态可以节省处理时间。

默认情况下，为所有服务器控件启用视图状态。若要禁用视图状态，请将控件的 EnableViewState 属性设置为 false，如下面的 DataGrid 服务器控件示例所示。

```
<asp:gridview EnableViewState="false" datasource="..."  runat="server"/>
```

还可以使用@ Page 指令禁用整个页的视图状态。当你不从页面回发到服务器时，这将十分有用：

```
<%@ Page EnableViewState="false" %>
```

注意@Control 指令中也支持 EnableViewState 属性，该指令允许你控制是否为用户控件启用视图状态。若要分析页上服务器控件使用的视图状态的数量，请（通过将 trace="true" 属性包括在@Page 指令中）启用该页的跟踪并查看 Control Hierarchy 表的 Viewstate 列。

（9）避免到服务器的不必要的往返过程。通常只有在查询或存储数据时才需要启动到服务器的往返过程。多数数据操作可在这些往返过程间的客户端上进行。例如，从 HTML 窗体验证用户输入可在数据提交到服务器之前在客户端进行。如果不需要将信息传递到服务器以将其存储在数据库中，那么你不应该编写导致往返过程的代码。

（10）使用 Page.IsPostBack 避免执行不必要的处理。例如下面的演示代码中在首次请求该页时将数据绑定到 GridView Web 控件中，以后刷新该页将不再绑定。

```
void Page_Load(Object sender, EventArgs e)
{
```

```
// Set up a connection and command here.
if (!Page.IsPostBack)
{
String query = "select * from Authors where FirstName like '%Tim%'";
myCommand.Fill(ds, "Authors");
myGridView.DataBind();
}
}
```

由于每次请求时都执行 Page_Load 事件，上述代码检查 IsPostBack 属性是否设置为 false。如果是，则执行代码。如果该属性设置为 true，则不执行代码。

（11）当不使用会话状态时禁用它。并不是所有的应用程序或页都需要针对于具体用户的会话状态，应该对任何不需要会话状态的应用程序或页禁用会话状态。若要禁用页的会话状态，请将@Page 指令中的 EnableSessionState 属性设置为 false。例如：

```
<%@ Page EnableSessionState="false" %>
```

注意：如果页需要访问会话变量，但不打算创建或修改它们，则将 @Page 指令中的 EnableSessionState 属性设置为 ReadOnly。若要禁用应用程序的会话状态，请在应用程序 Web.config 文件的 sessionstate 配置节中将 mode 属性设置为 off。例如：

```
<sessionstate mode="off" />
```

（12）仔细选择会话状态提供程序。ASP.NET 为存储应用程序的会话数据提供了三种不同的方法：进程内会话状态、作为 Windows 服务的进程外会话状态和 SQL Server 数据库中的进程外会话状态。每种方法都有自己的优点，但进程内会话状态是迄今为止速度最快的解决方案。如果只在会话状态中存储少量易失数据，则建议使用进程内提供程序。进程外解决方案主要用于跨多个处理器或多个计算机应用程序，或者用于服务器或进程重新启动时不能丢失数据的情况。

（13）不使用不必要的 Web 服务器控件。ASP.NET 中，大量的服务器端控件方便了程序开发，但也可能带来性能的损失，因为用户每操作一次服务器端控件，就产生一次与服务器端的往返过程。因此除非必要，应当少使用服务器端控件。

（14）优化 Web 服务器配置文件。默认情况下，ASP.NET 配置被设置成启用最广泛的功能并尽量适应最常见的方案。因此，应用程序开发人员可以根据应用程序所使用的功能，优化和更改其中的某些配置，以提高应用程序的性能。应仅对需要的应用程序启用身份验证。默认情况下的身份验证模式为 Windows。大多数情况下，对于需要身份验证的应用程序，最好在 Machine.config 文件中禁用身份验证，并在 Web.config 文件中启用身份验证。

根据适当的请求和响应编码设置来配置应用程序。ASP.NET 默认编码格式为 UTF-8。如果你的应用程序为严格的 ASCII，请配置应用程序使用 ASCII 以获得稍许的性能提高。

在 Machine.config 文件中将 AutoEventWireup 属性置为 false，意味着页面不将方法名与事件进行匹配并将两者挂钩（例如 Page_Load）。如果页面开发人员要使用这些事件，需要在基类中重写这些方法（例如需要为页面加载事件重写 Page_OnLoad，而不是使用

Page_Load 方法）。禁用 AutoEventWireup，页面将事件连接留给页面作者而不是自动执行它，将获得稍许的性能提升。

（15）缓存数据和页面输出。适当使用缓存可以更好地提高站点的性能，有时这种提高是非常明显的。使用 ASP.NET 缓存机制需要注意两点：首先不要缓存太多项，缓存每个项均有开销，特别是在内存使用方面，不要缓存容易重新计算和很少使用的项。其次给缓存的项分配的有效期不要太短。很快到期的项会导致缓存中不必要的周转，并且经常导致更多的代码清除和垃圾回收工作。若关心此问题，请监视与 ASP.NET Applications 性能对象关联的 Cache Total Turnover Rate 性能计数器。高周转率可能说明存在问题，特别是当项在到期前被移除时。这也称作内存压力。

11．ASP.NET 应用程序性能测试

在对 ASP.NET 应用程序进行性能测试之前，应确保应用程序没有错误，而且功能正常。性能测试工具 Web Application Stress Tool（WAS）是 Microsoft 发布的一个免费测试工具。它可以模拟成百上千个用户同时对 Web 应用程序进行访问请求，在服务器上形成流量负载，从而达到测试的目的，可以生成平均 TTFB、平均 TTLB 等性能汇总报告。另一个性能测试工具 Application Center Test（ACT）附带在 Microsoft Visual Studio.NET 的企业版中，是正式支持 Web 应用程序的测试工具，它能够直观地生成图表结果，功能比 WAS 多，但不具备多个客户机同时测试的能力。服务器操作系统“管理工具”中的“性能”计数器，可以对服务器进行监测以了解应用程序性能。

对于 Web 站点开发人员来说，在编写 ASP.NET 应用程序时注意性能问题，养成良好的习惯，可提高应用程序的性能。

8.8　Web 站点的安全性

计算机安全性涉及到的范围非常广泛。本节主要讨论如何保证 Web 站点安全运行的一般性方法。Web 站点安全性可从 Web 服务器的安全、数据库服务器的安全、Web 站点应用程序的安全三个方面来考虑。基于不同的环境配置的 Web 解决方案，其安全考虑各有侧重，但基本原则大致相同。下面我们以 Windows 平台为例来讨论 Web 站点的安全问题。

8.8.1　在安装 IIS 7.0 的服务器上应考虑的安全问题

（1）采用 NTFS 分区；尽可能安装操作系统的最新服务包和修补程序；增强口令的安全性；在网络配置中禁用 WINS、NETBIOS、LMHOST（用于 IP 地址与 Windows 计算机名称的映射）；停掉或卸载不必要的进程或服务。

（2）将磁盘上的默认 Web 站点位置从 c:\inetpub\更改到其他位置。

（3）使用 IIS 锁定工具（IIS Lockdown Tool）删除应用程序中未使用的所有其他动态内容类型，以缩小攻击者可用来攻击的区域。

（4）确保应用程序使用低权限的 ASP.NET 账户运行 ASP.NET 代码。

（5）将 ASP.NET 账户添加到 IIS 锁定工具创建的本地“Web 应用程序组”，以防进程运行任何未得到授权的命令行可执行程序。

（6）停掉默认的 Web 网站，新建一个网站作为 Web 应用程序站点，用虚拟目录来指定 Web 访问路径。

（7）配置 URLScan 2.5，使其只允许应用程序中使用的扩展集，并阻止较长的请求（URLScan 2.5 是由 IIS 锁定工具安装的，是一个 ISAPI 过滤器，可根据查询长度和字符集等规则监视和过滤发送到 IIS Web 服务器的所有输入请求）。

（8）设置 Web 内容目录的访问权限，授予 ASP.NET 进程对内容文件的读访问权限，授予匿名用户对所提供内容的适当只读访问权限。

（9）限制对 IIS 和 URLScan 的日志目录的访问，只有系统账户和系统管理员组才具有访问权限。

（10）安装防病毒软件和防木马软件等，启用计算机的防火墙功能。仅留必要的端口号。

（11）创建注册表项：nolmhash、NoDefault Exempt、Disable IPSource Routing、Syn Attack Protect 来提高系统安全性。

① 创建注册表项 nolmhash

nolmhash 在 Windows XP 和 Windows Server 2003 中，这是一个值。

位置：HKLM\System\Current ControlSet\Control\LSA

用途：防止操作系统以 LM 散列格式存储用户密码。此格式只用于不支持 NTLM 或 Kerberos 的 Windows 3.11 客户端。创建和保留此 LM 散列的风险在于，如果攻击者设法将以此格式存储的密码解密，就可以在网络上的其他计算机上重复利用这些密码。

② 创建注册表值 NoDefault Exempt

位置：HKLM\System\Current ControlSet\Services\IPSEC

用途：默认情况下，IPSec 将允许源端口为 88 的接入通信，查询 IPSec 服务，以获取连接到计算机的信息，而不管使用的是哪种 IPSec 策略。通过设置此值，除了我们设置的 IPSec 过滤器允许的通信以外，不允许端口之间进行任何通信。

③ 创建注册表值：Disable IPSource Routing

位置：HKLM\System\ CurrentControlSet\Services\Tcpip \Parameters

用途：防止 TCP 数据包显式确定到最终目标的路由，并防止它要求服务器确定最佳路由。这是一个防止“人在中间”攻击（即攻击者通过自己的服务器对数据包进行路由，并在数据包传递期间窃取其中的内容）的保护层。

④ 创建注册表值：Syn Attack Protect

位置：HKLM\System\Current ControlSet\Services\Tcpip\ Parameters

用途：此注册表项通过限制分配给传入请求的资源来防止操作系统受到某种 SYN-Flood 的攻击。换句话说，这将帮助阻止在客户端和服务器之间试图使用 SYN（即同步）请求以拒绝服务的攻击。

（12）通过对 Web 访问的日志进行审计，可以发现一些对安全方面有帮助的信息。

8.8.2 在安装 SQL Server 的服务器上应考虑的安全问题

（1）SQL Server 安装在 NTFS 分区上。

（2）为数据库访问建立替代账号，并为替代账号设置数据库访问角色，不要用 sa 账号。

（3）安装数据库系统的最新服务包。

（4）将数据库系统设置成禁用其他 SQL Server 通过 RPC 远程连接。

（5）选择低权限本地账户，启动 SQL Server 服务。

（6）停止 Distributed Transaction Coordinator（MSDTC）服务，并将其设置为手动启动。

（7）禁止数据库服务器运行 COM+ 应用程序。

（8）限制所支持的身份验证协议的级别（在“控制面板”|“管理工具”|“本地安全设置”|“安全设置”|“本地策略”|“安全选项”：LAN Manager 身份验证级别中进行设置）。

（9）禁用应用程序不需要的 SQL Server 代理和 Microsoft 搜索服务。

（10）设置 Server Network 的网络属性，由“直接客户端广播”改为“隐藏 SQL Server”。

（11）如应用程序不使用“命名管道”协议，则删除之。

（12）限制数据库用户只具有用得到的数据库操作权限。

（13）xp_cmdshell 是扩展存储过程，可以执行操作系统级命令，该存储过程的功能通过 SQL Server 安装目录中的文件 C:\Program Files\Microsoft SQL Server\MSSQL\Binn\xplog70.dll 获得，如果系统没有用到 xp_cmdshell 扩展存储过程，请将该文件换名或删除掉。

建议使用“金山漏洞修复”程序进行服务器的漏洞修复。

8.8.3　开发 Web 站点程序应考虑的安全性问题

（1）对 Web 应用系统应建立基于角色的用户权限管理机制。

（2）使用参数化存储过程。使用参数化存储过程是指在 Web 应用中，尽可能将对数据库的操作使用存储过程来完成，而不是动态构造 SQL 语句。将与数据库的交互限制到存储过程，这通常是增强 Web 安全的一个最佳方案。如果不存在存储过程，则 SQL 查询必须由 Web 应用程序动态构造。如果 Web 层遭到破坏，攻击者就可以向数据库查询中插入恶意命令，以检索、更改或删除数据库中存储的数据。使用存储过程，Web 应用程序与数据库的交互操作仅限于通过存储过程发送的几个特定的严格类型参数。每当开发人员使用.NET Framework 调用存储过程时，系统都会对发送到此存储过程的参数进行检查，以确保它们是存储过程可接受的类型（如整数、8 个字符的字符串等）。这是 Web 层有效性验证上的又一个保护层，可确保所有输入数据格式正确，且不能自行构造为可操作的 SQL 语句。

（3）输入有效性验证。输入有效性验证即是对所有用户输入的字符范围进行限制，以防可用于向 Web 站点发送恶意脚本的字符被禁止使用。通过 ASP.NET 的 System.Text.RegularExpressions.Regex 类提供的功能，用正则表达式对数据进行验证，例如：

```
Regex isNumber = new Regex("^[0-9]+$");
if(isNumber.Match(inputData) ) {
// 使用它
…
}
else {
// 丢弃它
…
}
```

正则表达式是用于匹配文本模式的字符和语法元素集合，用于确保查询字符串是正确且无恶意的。进行有效验证，防止用户在输入用户账号和密码的时候，输入"or 1=1"等可防止出现 SQL 注入攻击。

（4）尽量少用 session 和 application 变量，切忌不要通过 session 用来在页面间传递大数据量。定义的 session 变量如果不用，用 seesion.remove 从内存中释放掉，而不要让它等到超时释放。因为每个用户都要为 session 开辟存储区域，当访问用户量大的时候，服务器资源会很快耗尽。

（5）信息加密存储。信息加密存储是指对如数据库连接字符串、用户秘密等敏感信息进行加密存储，以妥善保护数据。数据库连接字符串存放有包括数据库服务器的位置、数据库名称和用户名以及密码等数据库连接信息，攻击者一旦设法读取字符串就可用它来访问数据库并对数据库进行恶意破坏。通常我们可以采用以下方法保护加密连接字符串等秘密信息：加密连接字符串，将其存储在注册表中，并使用访问控制列表（ACL）确保只有系统管理员和 ASP.NET 辅助进程才能访问注册表项。通过使用.NET Framework 的 System.Security.Cryptography 类中的 TripleDES 类提供的功能可实现对信息的加密。System.Security.Cryptography 加密算法主要分为：散列算法、对称加密算法、非对称加密算法。

（6）窗体身份验证。窗体身份验证即是当用户请求一个安全页面时，系统要对其进行判断，如果该用户已经登录系统并尚未超时，系统将返回此页面给请求用户；反之如该用户尚未登录，系统就要将此用户重定向到登录页面。

以上所述功能的实现只需对 Web.config 文件进行如下配置即可。

```
<authentication mode="Forms">
   <forms name="userInfo" loginUrl="login.aspx" protection="All">
   </forms>
</authentication>
<authorization>
    <deny users="?"/>
</authorization>
```

其中<authentication mode="Forms">用于身份验证。身份验证是在许可用户/应用程序访问某个资源之前验证客户端应用程序身份的过程。其中 mode 有 forms、passport、Windows、none 四种选择。<form></form>节中的 name 设置的是存储在客户端 Cookie 的名称，loginUrl 设置的是用户没有登录重定向的页面，protection 设置的是保护措施，有 All、none、encryption、validation 四个选项。All 选项设置执行验证和加密操作来保护 Cookie；none 选项对 Cookie 禁止加密和验证；encryption 选项对 Cookie 进行加密但不验证；validation 选项对 Cookie 验证但不加密。

<authorization>节表示在用户通过身份验证后，基于身份对该用户授予访问权限的过程。<deny>节中的 users 设置的是禁止的用户，“?”代表禁止匿名登录，“*”代表全体用户。与<deny>相对应的节还有<allow users>。在登录页面中添加如下代码：

```
If (与数据库的用户名密码字段比较判断用户是否合法)
{  System.Web.Security.FormsAuthentication.RedirectFromLoginPage(this.
```

```
TextBox1.Text, false);
  }
 else {
```

```
    Response.Write("身份不合法!");
}
```

对进行身份验证的登录页本身，应该采取两步方式验证用户存在且密码正确，且不可为图简便而使用一条 SQL 语句进行验证（如果攻击者攻破 Web 站点，并将 SQL 语句的 where 子句末尾加上一段永远为真的判断语句，则无论何时他都可以通过身份验证，这种攻击称为注入式攻击）。存在安全隐患的身份验证语句是：select * from users where name = namestr and password = passwdstr。比较安全的用户身份验证应该是：判断用户是否存在用“select name,password from users where name = namestr”。如用户存在，将返回一条包括用户名和密码的记录，然后判断由数据库返回的密码和用户输入的密码值：

```
if password = passwdstr {
//通过验证后的程序代码
…
}else{
//未通过验证后的程序代码
…
}
```

为加强用户名、密码等这些敏感信息在公网上的安全传输，应通过安全套接字层加密后再返回给 Web 服务器（例如使用 MD5，SHA1 对敏感信息进行加密）。

（7）通过在用户登录窗口中设置输入验证码的方法，可以防止非法用户以程序自动处理方式推测用户登录账户和密码，从而提高系统的安全性。验证码就是将一串随机产生的数字或符号，生成一幅图片，图片里加上一些干扰像素，由用户肉眼识别其中的验证码信息，输入表单后提交网站进行登录验证。

（8）在用户登录输入密码的时候，为防止木马程序非法录制按键操作，利用自定义软键盘让用户只能通过单击鼠标输入密码是目前很多银行网站采用的一种安全登录方式。

以上所介绍的是提高 Web 站点安全性的一般性方法，需要 Web 开发者根据应用系统的安全程度很好地规划和设计。

思考练习题

1．设计和开发一个 Web 站点需要注意哪些问题？
2．建设一个 Web 站点的一般步骤是什么？
3．进行网站开发时，应该从哪些方面来提高网站性能和安全性？