



21世纪高等院校规划教材

ASP 程序设计及应用

(第二版)

主 编 张景峰 庄连英
副主编 李 杰 张云峰 范 强



中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

在保留第一版易用、实用特点的同时,根据众多一线教师的反馈意见,对原书内容进行了认真的梳理,内容组织更加全面、实用,叙述更加准确、完整,力求适应目前培养应用型人才的需要。

全书共 11 章,内容包括 ASP 基础, Web 页面制作基础, VBScript 脚本语言, Response 与 Request 对象, Session、Application 和 Server 对象,文件系统操作, ASP 组件, Web 数据库基础, ADO 对象, 网上论坛系统和 Web 安全等。

本书既可作为本科院校计算机科学与技术专业及相关专业的教材,也可供广大有志于掌握 ASP 技术的人员使用。

本书配有电子教案,书中所有程序全部运行通过,读者可以从中国水利水电出版社网站及万水书苑上下载电子教案、源程序及相关文件,网址为: <http://www.waterpub.com.cn/softdown/>或 <http://www.wsbookshow.com>。也可以与作者(heblfzhang@163.com)联系获取所需资料。

图书在版编目(CIP)数据

ASP 程序设计及应用 / 张景峰, 庄连英主编. -- 2 版

— 北京: 中国水利水电出版社, 2012.1

21 世纪高等院校规划教材

ISBN 978-7-5084-9241-4

I. ①A… II. ①张… ②庄… III. ①网页制作工具—程序设计—高等学校—教材 IV. ①TP393.092

中国版本图书馆 CIP 数据核字(2011)第 258593 号

策划编辑: 雷顺加 责任编辑: 杨元泓 加工编辑: 刘晶平 封面设计: 李 佳

书 名	21 世纪高等院校规划教材 ASP 程序设计及应用(第二版)
作 者	主 编 张景峰 庄连英 副主编 李 杰 张云峰 范 强
出版发行	中国水利水电出版社 (北京市海淀区玉渊潭南路 1 号 D 座 100038) 网址: www.waterpub.com.cn E-mail: mchannel@263.net (万水) sales@waterpub.com.cn
经 售	电话: (010) 68367658 (发行部)、82562819 (万水) 北京科水图书销售中心(零售) 电话: (010) 88383994、63202643、68545874 全国各地新华书店和相关出版物销售网点
排 版	北京万水电子信息有限公司
印 刷	三河市鑫金马印装有限公司
规 格	184mm×260mm 16 开本 18.75 印张 459 千字
版 次	2005 年 3 月第 1 版第 1 次印刷 2012 年 1 月第 2 版 2012 年 1 月第 1 次印刷
印 数	0001—4000 册
定 价	32.00 元

凡购买我社图书,如有缺页、倒页、脱页的,本社发行部负责调换
版权所有·侵权必究

序

随着计算机科学与技术的飞速发展,计算机的应用已经渗透到国民经济与人们生活的各个角落,正在日益改变着传统的人类工作方式和生活方式。在我国高等教育逐步实现大众化后,越来越多的高等院校会面向国民经济发展的第一线,为行业、企业培养各级各类高级应用型专门人才。为了大力推广计算机应用技术,更好地适应当前我国高等教育的跨越式发展,满足我国高等院校从精英教育向大众化教育的转变,符合社会对高等院校应用型人才培养的各类要求,我们成立了“21世纪高等院校规划教材编委会”,在明确了高等院校应用型人才培养模式、培养目标、教学内容和课程体系的框架下,组织编写了本套“21世纪高等院校规划教材”。

众所周知,教材建设作为保证和提高教学质量的重要支柱及基础,作为体现教学内容和教学方法的知识载体,在当前培养应用型人才中的作用是显而易见的。探索和建设适应新世纪我国高等院校应用型人才培养体系需要的配套教材已经成为当前我国高等院校教学改革和教材建设工作面临的紧迫任务。因此,编委会经过大量的前期调研和策划,在广泛了解各高等院校的教学现状、市场需求,探讨课程设置、研究课程体系的基础上,组织一批具备较高的学术水平、丰富的教学经验、较强的工程实践能力的学术带头人、科研人员和主要从事该课程教学的骨干教师编写出一批有特色、适用性强的计算机类公共基础课、技术基础课、专业及应用技术课的教材以及相应的教学辅导书,以满足目前高等院校应用型人才培养的需要。本套教材消化和吸收了多年来已有的应用型人才培养的探索与实践成果,紧密结合经济全球化时代高等院校应用型人才培养工作的实际需要,努力实践,大胆创新。教材编写采用整体规划、分步实施、滚动立项的方式,分期分批地启动编写计划,编写大纲的确定以及教材风格的定位均经过编委会多次认真讨论,以确保该套教材的高质量和实用性。

教材编委会分析研究了应用型人才与研究型人才在培养目标、课程体系和内容编排上的区别,分别提出了3个层面上的要求:在专业基础类课程层面上,既要保持学科体系的完整性,使学生打下较为扎实的专业基础,为后续课程的学习做好铺垫,更要突出应用特色,理论联系实际,并与工程实践相结合,适当压缩过多过深的公式推导与原理性分析,兼顾考研学生的需要,以原理和公式结论的应用为突破口,注重它们的应用环境和方法;在程序设计类课程层面上,把握程序设计方法和思路,注重程序设计实践训练,引入典型的程序设计案例,将程序设计类课程的学习融入案例的研究和解决过程中,以学生实际编程解决问题的能力为突破口,注重程序设计的算法的实现;在专业技术应用层面上,积极引入工程案例,以培养学生解决工程实际问题的能力为突破口,加大实践教学内容的比重,增加新技术、新知识、新工艺的内容。

本套规划教材的编写原则是:

在编写中重视基础,循序渐进,内容精炼,重点突出,融入学科方法论内容和科学理念,反映计算机技术发展要求,倡导理论联系实际和科学的思想方法,体现一级学科知识组织的层次结构。主要表现在:以计算机学科的科学体系为依托,明确目标定位,分类组织实施,兼容互补;理论与实践并重,强调理论与实践相结合,突出学科发展特点,体现学科发展的内在规律;教材内容循序渐进,保证学术深度,减少知识重复,前后相互呼应,内容编排合理,整体

结构完整；采取自顶向下设计方法，内涵发展优先，突出学科方法论，强调知识体系可扩展的原则。

本套规划教材的主要特点是：

(1) 面向应用型高等院校，在保证学科体系完整的基础上不过度强调理论的深度和难度，注重应用型人才的专业技能和工程实用技术的培养。在课程体系方面打破传统的研究型人才培养体系，根据社会经济发展对行业、企业的工程技术需要，建立新的课程体系，并在教材中反映出来。

(2) 教材的理论知识包括了高等院校学生必须具备的科学、工程、技术等方面的要求，知识点不要求大而全，但一定要讲透，使学生真正掌握。同时注重理论知识与实践相结合，使学生通过实践深化对理论的理解，学会并掌握理论方法的实际运用。

(3) 在教材中加大能力训练部分的比重，使学生比较熟练地应用计算机知识和技术解决实际问题，既注重培养学生分析问题的能力，也注重培养学生思考问题、解决问题的能力。

(4) 教材采用“任务驱动”的编写方式，以实际问题引出相关原理和概念，在讲述实例的过程中将本章的知识点融入，通过分析归纳，介绍解决工程实际问题的思想和方法，然后进行概括总结，使教材内容层次清晰，脉络分明，可读性、可操作性强。同时，引入案例教学和启发式教学方法，便于激发学习兴趣。

(5) 教材在内容编排上，力求由浅入深，循序渐进，举一反三，突出重点，通俗易懂。采用模块化结构，兼顾不同层次的需求，在具体授课时可根据各校的教学计划在内容上适当加以取舍。此外还注重了配套教材的编写，如课程学习辅导、实验指导、综合实训、课程设计指导等，注重多媒体教学方式以及配套课件的制作。

(6) 大部分教材配有电子教案，以使教材向多元化、多媒体化发展，满足广大教师进行多媒体教学的需要。电子教案用 PowerPoint 制作，教师可根据授课情况任意修改。相关教案的具体情况请到中国水利水电出版社网站 www.waterpub.com.cn 下载。此外还提供相关教材中所有程序的源代码，方便教师直接切换到系统环境中教学，提高教学效果。

总之，本套规划教材凝聚了众多长期在教学、科研一线工作的教师及科研人员的教学科研经验和智慧，内容新颖，结构完整，概念清晰，深入浅出，通俗易懂，可读性、可操作性和实用性强。本套规划教材适用于应用型高等院校各专业，也可作为本科院校举办的应用技术专业的课程教材，此外还可作为职业技术学院和民办高校、成人教育的教材以及从事工程应用的技术人员的自学参考资料。

我们感谢该套规划教材的各位作者为教材的出版所做出的贡献，也感谢中国水利水电出版社为选题、立项、编审所做出的努力。我们相信，随着我国高等教育的不断发展和高校教学改革的不深入，具有示范性并适应应用型人才培养的精品课程教材必将进一步促进我国高等院校教学质量的提高。

我们期待广大读者对本套规划教材提出宝贵意见，以便进一步修订，使该套规划教材不断完善。

第二版前言

《ASP 程序设计及应用》一书自 2005 年 3 月出版以来已发行了 2 万余册,受到了广大读者的欢迎,已经在多所高校中得到了使用。随着技术的进步和使用的普及,迫切需要对原书进行修订。

《ASP 程序设计及应用》(第二版)在保留第一版易用、实用特点的同时,根据众多一线教师的反馈意见,对原书内容进行了认真的梳理,内容组织更加全面、实用,叙述更加准确、完整,力求适应目前培养应用型人才的需要。

与第一版相比,本书做了较大的改动,主要体现在以下几个方面:

(1) 第 2 章“Web 页面制作基础”中,在保留第一版中 HTML 标记的内容外,对 CSS、DIV 等方面的知识点做了一定的强化,并加入了 XML 的内容。

(2) 对章节的编排做了较大的改动。将第一版中的第 5 章“Session 和 Application 对象”和第 6 章“Server 和ObjectContext 对象”合并为一章,将第 10 章“ADO 对象”和第 11 章“Web 数据库的操作”合并为一章,避免了知识点过于分散、不利于学生掌握的不足。

(3) 考虑目前后台数据库的使用情况,对第一版的数据库进行了升级,以 Access 2003 和 SQL Server 2005 数据库系统作为重点,详细说明了在 ASP 中对其操作的全过程。

(4) 对第一版中的实例做了一些修改,力求针对性强、实用性高;同时结合目前 ASP 的实际应用,重写了第一版中最后章节的实例,以期达到巩固、加深全书知识点的效果。

(5) 第 11 章“Web 安全”是新增的内容。从 Web 服务器安全、网页木马、SQL 注入攻击与防范和跨站脚本攻击 4 个方面做了较为详细的介绍。

(6) 为便于教师组织教学,除了在每章设置了“思考题”外,还针对各章节的内容设计了“上机实验”。

本书由张景峰、庄连英主编,李杰、张云峰、范强担任副主编。各章编写分工如下:第 1、4、5、8 章由张景峰编写,第 2、3 章由庄连英编写,第 6、7 章由李杰编写,第 9 章由范强编写,第 10 章由王培军编写,第 11 章由张云峰编写。参加本书编写大纲讨论的还有翟智平、张凯等。此外,王智华、徐建新、陈晓红、郭冬滨等参与了本书的校对工作。

本书是集体智慧的结晶,作者均是使用过本书第一版为学生多次授课的一线教师,对书中内容有较深的体会,很多修改思路来自于教学、科研实践。书中保留了第一版中的精华,由于各种原因,一部分原书作者没有参与本次改版工作,但他们对本书的贡献不可磨灭,在此对韩红旗、刘博涛等第一版作者表示深深的谢意。

在本书的编写过程中,参考了大量的相关技术资料,吸取了许多同仁的宝贵经验,在此深表谢意。尽管已经尽了最大的努力来避免错误的发生,但限于时间和水平,书中不妥和错误在所难免,恳请各位专家、读者批评指正。编者的 E-mail 为:heblfzhang@163.com。

编 者

2011 年 12 月

第一版前言

ASP 是开发 Web 应用程序非常有效的一项技术，由于其具有功能强大、易于开发和修改的特点，目前已经得到了广泛的应用。ASP 既不是一种语言，也不是一种开发工具，而是一种技术框架，其主要功能是把脚本、HTML、组件和 Web 数据库访问功能有机地结合在一起，形成一个能在服务器端运行的交互、动态且高效的 Web 应用程序。

本书从实用的角度出发，按照教学规律，由浅入深、循序渐进地介绍了与 ASP 开发相关的技术细节。全书共 12 章：第 1 章介绍 ASP 的基础知识，包括静态网页和动态网页的执行过程，Web 服务器的设置以及 ASP 程序的编写和运行；第 2 章介绍常用的 HTML 标记以及 CSS 的基础知识；第 3 章介绍客户端脚本与服务器端脚本的概念以及 VBScript 脚本语言；第 4~6 章是本书的重点，主要介绍 ASP 的 6 个内置对象：Request、Response、Session、Application、Server 和 ObjectContext 对象，在对这些对象的具体描述中设置了大量的实例，以期达到巩固、加深所学知识的目的；第 7 章介绍如何在 ASP 中使用组件，这些组件既包括 ASP 的内置组件，也包括其他第三方提供的组件；第 8 章具体介绍文件组件的使用方法；第 9~11 章介绍利用 ASP 开发 Web 数据库的内容，考虑到这部分内容具有极高的使用价值，相关知识点的叙述较为完整，从数据库的建立、ODBC 数据源的设置、ADO 对象的使用到实际开发中应该掌握的技巧都作了必要的阐述；第 12 章结合门诊信息管理系统、网页“换肤”、新闻发布系统、网上考试管理系统等 4 个实际使用的实例，以便读者加深对本书所述内容的理解。

为了使读者能够快速掌握利用 ASP 开发 Web 应用程序的技术，本书作者结合多年的教学及科研经验，按照教材的体例编写了本书。在编写过程中力求内容翔实、便于教学；在具体内容的描述中力求叙述准确、通俗易懂。

本书由张景峰主编，韩红旗、刘博涛任副主编。各章编写分工如下：第 1、4 章由韩红旗编写，第 2、3 章由庄连英编写，第 5 章和第 8 章由刘博涛编写，第 6、7、9、10 和 11 章由张景峰编写，第 12 章由王培军、刘博涛、庄连英共同编写。参加本书编写大纲讨论的还有苏英如、李伟红、张保通、刘永华、潘明寒、雨轩、雷先胜、张浩军、王红等。此外，韩煜、邹彭涛、王振夺、史建芳、朱越、周晓聪等参与了本书的校对工作。

在本书的编写过程中，参考了大量的相关技术资料，吸取了许多同仁的宝贵经验，在此深表谢意。尽管已经尽了最大的努力来避免错误的发生，但限于时间和水平，书中不妥和错误在所难免，恳请各位专家、读者批评指正。编者的 E-mail 为：zhangjf@nciae.edu.cn。

编 者

2005 年 1 月

目 录

序

第二版前言

第一版前言

第1章 ASP 基础	1	2.4 制作表格	27
本章学习目标	1	2.4.1 建立表格	27
1.1 Web 基础	1	2.4.2 定制表格	27
1.1.1 Web 概述	1	2.5 制作表单	29
1.1.2 Web 工作原理	2	2.5.1 表单的结构	29
1.1.3 静态网页与动态网页	3	2.5.2 FORM 中常用的标记	30
1.1.4 交互式动态网页实现技术简介	6	2.6 框架结构	34
1.2 ASP 概述	7	2.6.1 框架结构的文件格式	34
1.2.1 ASP 的特点	7	2.6.2 框架结构标记的使用	35
1.2.2 ASP 文件的基本结构	7	2.6.3 FRAME 标记	35
1.3 ASP 的运行	8	2.6.4 TARGET 属性的使用	36
1.3.1 IIS 5.1 的安装	9	2.7 CSS 基础	37
1.3.2 IIS 5.1 的设置	9	2.7.1 CSS 样式简介	37
1.3.3 ASP 的运行	12	2.7.2 CSS 样式表的定义	38
思考题	13	2.7.3 在 HTML 中加入 CSS 的方法	41
上机实验	14	2.8 XML 基础	42
第2章 Web 页面制作基础	15	2.8.1 XML 简介	42
本章学习目标	15	2.8.2 XML 文档的结构	42
2.1 HTML 语言概述	15	2.8.3 XML 语法规则	43
2.1.1 HTML 概述	15	2.8.4 XML 元素和属性的对比	44
2.1.2 HTML 文档的结构	16	2.8.5 XML 在 HTML 中的应用	44
2.1.3 HTML 标记	16	思考题	46
2.1.4 常用 HTML 编辑工具	17	上机实验	46
2.2 文档的格式与风格	17	第3章 VBScript 脚本语言	47
2.2.1 设置<BODY>的属性	18	本章学习目标	47
2.2.2 段落格式化	18	3.1 VBScript 脚本语言概述	47
2.2.3 建立列表	22	3.1.1 服务器端脚本和客户端脚本	47
2.2.4 字符的格式化	24	3.1.2 VBScript 脚本语言编程实例	48
2.3 加入多媒体与超级链接	25	3.1.3 VBScript 和 JavaScript	51
2.3.1 加入图像、视频、动画	25	3.2 基本数据类型及输入/输出	51
2.3.2 加入超级链接	26	3.2.1 将单行语句分成多行	51

3.2.2 在代码中加注释	52	4.3.1 Request 对象的属性	97
3.2.3 使用不同进制的数字	52	4.3.2 Request 对象的方法	97
3.2.4 数据类型及其子类型	53	4.3.3 Request 对象的数据集合	97
3.2.5 变量	54	4.4 综合实例	107
3.2.6 常量	56	4.4.1 创建登录页面	107
3.2.7 数组	57	4.4.2 用户验证	108
3.2.8 基本输入输出	58	思考题	110
3.3 表达式和运算符	62	上机实验	110
3.3.1 VBScript 的表达式	62	第 5 章 Session、Application 和 Server 对象	112
3.3.2 VBScript 的数学表达式及其运算符	62	本章学习目标	112
3.3.3 VBScript 的条件表达式及其运算符	63	5.1 Session 对象	112
3.3.4 VBScript 的字符串表达式	64	5.1.1 Session 概述	112
3.3.5 表达式中的优先级	65	5.1.2 Session 对象的数据集合	113
3.4 VBScript 中的控制语句	65	5.1.3 Session 对象的属性	116
3.4.1 控制语句	65	5.1.4 Session 对象的方法	117
3.4.2 条件控制语句	66	5.1.5 Session 对象的事件	118
3.4.3 循环控制语句	69	5.2 Application 对象	119
3.4.4 其他常用简单语句	73	5.2.1 Application 对象概述	119
3.5 VBScript 函数及子过程	74	5.2.2 Application 对象的集合	119
3.5.1 过程	74	5.2.3 Application 对象的方法	122
3.5.2 子过程	74	5.2.4 Application 对象的事件	122
3.5.3 函数	75	5.2.5 Global.asa 文件	123
3.5.4 Exit 语句	76	5.3 Server 对象	125
3.5.5 VBScript 内部函数摘要	76	5.3.1 Server 对象的属性	125
3.6 VBScript 的对象和事件	79	5.3.2 Server 对象方法	125
3.6.1 对象和事件的概念	79	5.4 网上聊天室	128
3.6.2 网页及浏览器对象	79	5.4.1 Global.asa 文件	129
3.6.3 浏览器内嵌 HTML 控件	81	5.4.2 用户登录	129
3.6.4 对象和事件实例	82	5.4.3 聊天室主页	131
思考题	84	5.4.4 改进的聊天室	134
上机实验	84	思考题	134
第 4 章 Response 与 Request 对象	85	上机实验	135
本章学习目标	85	第 6 章 文件系统操作	136
4.1 ASP 内置对象	85	本章学习目标	136
4.2 Response 对象	86	6.1 文件操作对象	136
4.2.1 Response 对象的属性	86	6.2 文件及文件夹处理	137
4.2.2 Response 对象的方法	89	6.2.1 FileSystemObject 对象	137
4.2.3 Response 对象的数据集合	94	6.2.2 复制、移动及删除文件	139
4.3 Request 对象	96	6.2.3 文件夹处理	140

6.3 文本文件的读写操作	142	8.2.3 创建空白数据表	170
6.3.1 TextStream 对象	142	8.2.4 设置表的主键	170
6.3.2 读取文本文件中的数据	142	8.2.5 操作表中的数据	171
6.3.3 对文本文件的写操作	144	8.3 SQL Server 2005 基础	171
6.4 计数器实例	145	8.3.1 SQL Server 2005 简介	171
6.4.1 用文件实现的计数器	145	8.3.2 创建数据库	173
6.4.2 用文件及图形实现的综合计数器	147	8.3.3 创建数据表	175
思考题	148	8.3.4 设置表的主键	175
上机实验	148	8.3.5 操作表中的数据	175
第 7 章 ASP 组件	149	8.4 SQL 语言基础	175
本章学习目标	149	8.4.1 SQL 简介	175
7.1 ASP 组件概述	149	8.4.2 查询表中的数据信息	176
7.2 Ad Rotator 组件	149	8.4.3 编辑数据库中的数据	179
7.2.1 Ad Rotator 组件的属性和方法	150	思考题	180
7.2.2 Ad Rotator 组件相关文件	151	上机实验	180
7.3 Browser Capabilities 组件	153	第 9 章 ADO 对象	182
7.3.1 Browscap.ini 文件	154	本章学习目标	182
7.3.2 Browser Capabilities 组件的使用	156	9.1 ADO 概述	182
7.4 Content Linking 组件	157	9.1.1 ASP 访问数据库的方法	182
7.4.1 线性排列顺序文件	157	9.1.2 ODBC 的设置	183
7.4.2 Content Linking 组件的方法	157	9.1.3 ADO 中的对象和数据集合	187
7.5 计数器组件	159	9.2 Connection 对象	189
7.5.1 计数器组件的方法	160	9.2.1 Connection 对象的方法	189
7.5.2 计数器组件的使用	160	9.2.2 Connection 对象的属性	195
7.6 CDONTS 组件	160	9.2.3 Connection 对象的数据集合	197
7.6.1 CDONTS 组件的属性和方法	161	9.3 Command 对象	201
7.6.2 CDONTS 组件的使用	161	9.3.1 Command 对象的属性	201
7.7 ASPUpload 组件	163	9.3.2 Command 对象的方法	202
7.7.1 ASPUpload 组件的常用属性和方法	163	9.3.3 Command 对象的数据集合	204
7.7.2 ASPUpload 组件的使用	164	9.3.4 调用存储过程	207
7.8 其他 ASP 组件	166	9.4 RecordSet 对象	210
思考题	167	9.4.1 RecordSet 对象的属性	210
上机实验	167	9.4.2 RecordSet 对象的数据集合	217
第 8 章 Web 数据库基础	168	9.4.3 RecordSet 对象的方法	218
本章学习目标	168	9.5 ADO 对象综合应用	227
8.1 关系数据库概述	168	9.5.1 分页显示	227
8.2 Access 2003 基础	169	9.5.2 修改数据	229
8.2.1 Access 2003 简介	169	9.5.3 删除多条记录	233
8.2.2 创建空数据库	169	思考题	235

上机实验	235	10.7.1 模块功能描述	257
第 10 章 网上论坛系统	236	10.7.2 话题搜索页	257
本章学习目标	236	10.8 论坛管理功能模块	260
10.1 网上论坛需求分析和说明	236	10.8.1 模块功能描述	260
10.2 软件设计和功能模块划分	236	10.8.2 论坛管理主页面	260
10.3 编写程序代码	237	10.8.3 论坛管理执行页	263
10.3.1 程序代码文件的存放位置	237	思考题	268
10.3.2 数据库和 ODBC 数据源的创建	237	上机实验	268
10.3.3 论坛系统 Web 站点的创建	237	第 11 章 Web 安全	269
10.3.4 层叠样式表文件 global.css	237	本章学习目标	269
10.3.5 公用函数文件 conn_db.asp	238	11.1 Web 服务器安全	269
10.3.6 编辑 global.asa 文件	238	11.1.1 Web 服务器安全漏洞	269
10.4 用户注册、登录和注销功能模块	239	11.1.2 操作系统的安全配置	269
10.4.1 模块功能描述	239	11.1.3 Web 服务器软件 IIS 的安全配置	272
10.4.2 用户信息表 user_info	239	11.2 网页木马	273
10.4.3 用户注册	240	11.3 SQL 注入攻击与防范	277
10.4.4 用户登录	242	11.3.1 SQL 注入攻击简介	277
10.4.5 用户注销	243	11.3.2 SQL 注入攻击特点	277
10.5 话题管理功能模块	243	11.3.3 SQL 注入攻击实现过程	278
10.5.1 模块功能描述	243	11.3.4 寻找 SQL 注入点	278
10.5.2 话题信息表 art_info	244	11.3.5 获取信息和实施攻击	280
10.5.3 发表新话题	244	11.3.6 SQL 注入攻击检测	281
10.5.4 修改话题	245	11.3.7 SQL 注入攻击的防范	281
10.5.5 删除话题	247	11.4 跨站脚本攻击	283
10.6 论坛栏目信息模块	247	11.4.1 跨站攻击简介	283
10.6.1 模块功能描述	247	11.4.2 XSS 攻击的危害	285
10.6.2 栏目信息表 column_info	247	11.4.3 XSS 攻击分类	285
10.6.3 论坛主页面 main_bbs.asp	248	11.4.4 XSS 攻击的防范	286
10.6.4 栏目主页面	250	思考题	286
10.6.5 话题内容页面	253	上机实验	287
10.7 论坛话题搜索功能模块	257	参考文献	288

第 1 章 ASP 基础

本章学习目标

本章主要介绍 ASP 的基础知识。通过本章的学习，读者应该掌握以下内容：

- Web 基本概念及工作原理
- 静态网页与动态网页的概念及执行过程
- ASP 的特点及 ASP 文件的基本结构
- IIS 5.1 的安装与设置
- ASP 文件的基本结构和运行方法

1.1 Web 基础

随着现代社会人们对信息的极大需求和计算机网络技术的高速发展，Internet 已经成为一个信息传播的重要平台。越来越多的人习惯于通过 Internet 获取需要的信息，相当数量的企业和个人已经或正在利用这个平台方便、快捷地发布信息，Internet 已经成为继报纸、电台、电视这些传统的媒体后又一个重要的信息传输媒体。

Internet（因特网）又称为国际互联网、因特网、网际网或信息高速公路等，它是将不同地区而且规模大小不一的网络互相连接而成，是当今世界上最大的计算机网络。目前 Internet 上可以提供的服务种类非常多，如远程登录 Telnet、电子邮件 E-mail、文件传输 FTP、万维网 Web 等，其中 Web 和 E-mail 是最常用的服务。

1.1.1 Web 概述

Web（World Wide Web 或 WWW、3W，万维网）并非某种特殊的计算机网络，而是一个规模巨大的、分布式的信息储藏所。Web 的出现，使 Internet 从原来仅由少数专业人士使用转变为普通用户也能利用的信息资源，是 Internet 发展中一个重要的里程碑。

Web 是一种基于超级链接（HyperLink）技术的分布式的超媒体（HyperMedia）系统，是对超文本（HyperText）系统的扩充。超媒体与超文本的区别在于文档的内容不同：超文本文档仅包含文本信息，而超媒体文档还可包含诸如图形、图像、音频、视频等其他表示方式的信息。

在 Web 系统中，信息的表示和传送一般使用 HTML（Hyper Text Markup Language，超文本标记语言）格式，利用这种格式描述的信息可以为用户提供一个易于使用的、包含超媒体信息的图形化界面。

Web 系统还具有极强的超级链接能力。利用超级链接技术，Web 系统将位于不同网络位置的文件之间建立了联系，用户通过单击不同的超级链接就可以方便地访问指定的资源，为用

户提供了一种交叉式（而非线性）的访问资源的方式。

由于 Web 具有极强的易用性和实用性，普通的 Internet 用户可以方便地利用 Web 系统访问 Internet 上丰富多彩的资源，目前已经成为 Internet 上使用最为广泛、最有前途、最受欢迎的信息服务工具之一，是 Internet 上发布信息的主要手段。

1.1.2 Web 工作原理

Web 是基于客户/服务器的一种体系结构。一般来说，用户的计算机称为 Web 客户机，用于提供 Web 服务的计算机称为 Web 服务器。浏览器就是在用户计算机上的 Web 客户程序，它负责发出 Web 请求，并接收 Web 服务器的响应，目前常用的浏览器有 Firefox(火狐狸)和 Internet Explorer (IE)。Web 服务器负责响应客户机的请求，需要安装 Web 服务器软件，常见的软件有 Microsoft Internet Information Server (IIS) 和 Apache HTTP Server 等。

1. HTTP 协议

HTTP (HyperText Transfer Protocol, 超文本传输协议) 是一种非常重要的 WWW 传输协议。它限制了在网络中传输信息的内容以及 Web 客户机与 Web 服务器之间交互的方式。目前普遍使用的是 HTTP 1.1 协议，HTTP 1.1 比 HTTP 1.0 传输效率更高，支持断点续传和管道连接。

当 Web 客户机从一个 Web 服务器接收 HTML 文件时，就会使用 HTTP 协议。首先，浏览器会建立一个到网站的连接并发出一个请求，服务器在接受请求并进行相应的处理后，将发出一个响应（通常这个响应是一个 Web 页面），客户机将得到的响应解释并显示出来，最后关闭前面建立的连接。Web 的这种资源访问机制又被称为 B/S (Browser/Server, 浏览器/服务器) 模式，其工作过程如图 1-1 所示。

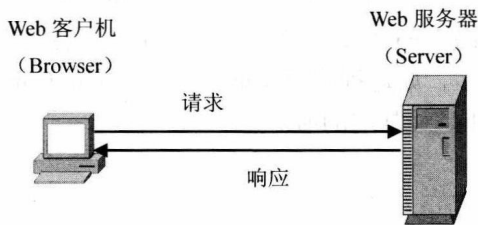


图 1-1 Web 资源访问机制

在 HTTP 中，所有从 Web 客户机到 Web 服务器的通信都是分开的请求和响应对，是各自独立的。Web 客户机总是首先发送请求初始化这种通信过程，Web 服务器被动地做出响应。

2. URL

URL (Uniform Resource Locator, 统一资源定位符) 用于在 Internet 上唯一地标识每个资源地址和获取资源的方式，通常也称为 URL 地址、网站地址或网址。Web 客户机就是依靠 URL 来访问指定的 Web 服务器的。

一个 URL 类似于物理的树型地址，由以冒号分隔的两大部分组成，在 URL 中的字符不区分大小写。URL 的一般格式为：

<URL 的访问方式>://<主机名>:<端口>/<路径>/.../文件名

其中 URL 的访问方式指定访问特定资源时应使用的 Internet 协议，常用的有 HTTP (超文

本传输协议)、FTP (文件传输协议)、Telnet (远程登录服务)、Mailto (电子邮件)、File (本地文件) 等。如果不指定协议, 默认使用 HTTP 协议。

主机名指定 Web 服务器的 IP 地址或域名地址, 如 `www.microsoft.com` 或 `210.31.224.1`。

端口指明了 Internet 服务的端口号。端口段不是必填项, 通常 Internet 用户不需要指定, 而采用默认的端口号, 如 HTTP 协议默认的端口号为 80。只有在服务器不使用默认端口提供服务时才有必要在 URL 中输入指定的端口。

路径指定要访问的文件在 Internet 服务器上的位置, 每一级目录以一个正斜杠 (/) 符号隔开。

文件名是将要访问的文件名称, 包括主文件名和扩展名, 如 `index.html`。

一个完整的 URL 地址如下:

`http://www.baidu.com:80/index.html`

在 URL 中端口、目录、文件名对于定位要访问的资源来说是很重要的, 但不是必需的。所有的 URL 最少必须包含 URL 的访问方式和主机名。当没有指定路径和文件名时, 表示要访问该服务器的默认文档, 举例如下:

`http://www.baidu.com/`

1.1.3 静态网页与动态网页

当 Web 客户机提出页面请求后, Web 服务器经过某些处理后会给出相应的响应。根据 Web 服务器上处理方式的不同, 可以将网页分为静态网页与动态网页。

1. 静态网页

静态网页是标准的 HTML 文件, 其文件扩展名为 `.htm` 或 `.html`, 它可以包含文本、HTML 标记、客户机脚本及客户机 ActiveX 控件等, 举例如下 (文件名为 `thefirst.htm`)。

例 1-1:

```
<HTML>
<HEAD>
<TITLE>HTML 页面示例</TITLE>
</HEAD>
<BODY>
<FONT SIZE=7>第一个页面</FONT>
</BODY>
</HTML>
```

说明: HTML 文件是一个纯文本文件, 可以使用任何一种文本编辑器 (如 Windows 中的记事本、写字板等) 创建。

任何 Web 服务器都支持静态网页, 其执行过程如下:

(1) 当用户在浏览器的地址栏中输入要访问的 URL 地址并按回车键或单击 Web 页上的某个超级链接时, 浏览器向 Web 服务器发送一个页面请求。

(2) Web 服务器接收到这些请求, 根据扩展名 `.htm` 或 `.html` 判断出请求的是 HTML 文件, 然后服务器从当前硬盘或内存中读取正确的 HTML 文件, 将它送回用户浏览器。

(3) 用户的浏览器解释这些 HTML 文件, 并将结果显示出来。

静态网页的执行过程如图 1-2 所示。

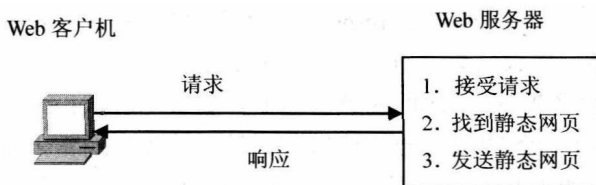


图 1-2 静态网页的执行过程

从上述描述中可以看出, Web 服务器在静态网页的执行过程中占有重要的地位, 这与在硬盘中双击某个 HTML 文件有着本质的区别 (双击文件并没有经过 Web 服务器)。请读者仔细体会这种区别。

静态网页中显示的内容在用户访问之前就已经完全确定了, 不论何时, 任何用户访问该页面都会得到相同的显示效果。例如, 所有访问 <http://www.google.cn/> 网站的用户都会在浏览器中得到如图 1-3 所示的结果。



图 1-3 Google 网站首页

需要说明的是, 即使该页面包含一些视频动画, 由于浏览器的显示结果相同, 也被认为是静态网页。

由于静态网页不能根据用户的需要, 动态地访问 Web 服务器上的信息, 因此与用户之间缺少交互性; 此外, 静态页面不支持对数据库的操作, 只能用来制作一些内容固定的页面; 如果要修改静态页面的内容, 只能修改 Web 服务器上该页面的源代码, 页面的后期维护工作量较大。为了使网站更加有效地工作, 满足用户对信息的需求, 还应该在网站中采用动态网页技术。

2. 动态网页及其执行过程

动态网页中除包含有静态网页中可以出现的内容外, 还可以包含只能在 Web 服务器上运行的服务器端脚本。动态网页文件的扩展名与所使用的 Web 应用开发技术有关。例如, 使用 ASP 技术时文件扩展名为 .asp, 使用 PHP 技术时文件扩展名为 .php, 使用 JSP 技术时文件扩展名为 .jsp。

动态网页的执行过程如下:

(1) 当用户在浏览器的地址栏中输入要访问的 URL 地址并按回车键或单击 Web 页上的某个超级链接时, 浏览器将这个动态网页的请求发送到 Web 服务器。

(2) Web 服务器接收这些请求并根据扩展名 (如.asp) 判断请求的是动态网页文件, 服务器从硬盘或内存中读取相应的文件。

(3) Web 服务器将这个动态网页文件从头至尾执行, 并根据执行结果生成相应的 HTML 文件 (静态网页)。

(4) HTML 文件被送回浏览器, 浏览器解释这些 HTML 文件并将结果显示出来。
动态网页的执行过程如图 1-4 所示。

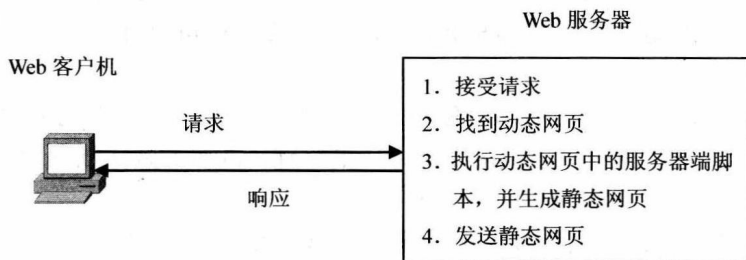


图 1-4 动态网页的执行过程

上述过程是一个简化的过程, 但从中可以看出动态网页与静态网页有着本质的区别。对于 Web 服务器来说, 静态网页不经过任何处理就被送到了客户机浏览器, 而动态网页中的内容首先要在服务器端执行, 并根据执行结果生成相应的 HTML 页面, 再将 HTML 页面送给客户机浏览器。也就是说, 动态页面具有很强的交互性, 可以根据用户的不同选择执行不同的代码、显示不同的内容。例如, 在 www.google.cn 网站上搜索 “ASP” 时, 会得到如图 1-5 所示的结果。



图 1-5 www.google.cn 上搜索 “ASP” 得到的结果

当不同的用户搜索不同的内容时, 其浏览器中会有不同的显示, 实现了网页内容的动态显示。

由于动态网页必须在 Web 服务器端执行, 因此, 双击硬盘中的动态网页文件时, 只能看

到该文件的源代码,而看不到该文件的执行结果。

1.1.4 交互式动态网页实现技术简介

目前实现交互式动态网页的技术主要有 CGI、ASP、JSP、PHP 和 ASP.NET 等。

1. CGI

CGI (Common Gateway Interface, 通用网关接口) 是外部程序和 Web 服务器之间的标准编程接口。可以使用各种不同的程序语言编写适合的 CGI 程序,这些程序语言包括 Visual Basic、Delphi 或 C/C++ 等,可以将已经写好的程序放在 Web 服务器的计算机上运行,再将其运行结果通过 Web 服务器传输到客户端的浏览器上。事实上,这样的编制方式比较困难而且效率低,因为每一次修改程序都必须重新将 CGI 程序编译成可执行文件。

2. ASP

ASP (Active Server Pages, 活动服务器网页), 由于其应用程序具有容易开发和修改、功能强大等特点,一经推出就受到了众多专业人士的好评,再加上微软强有力的支持,可以说是时下动态网页开发技术中最为流行的技术之一。

可以认为 ASP 是一种类似于 HTML、脚本与 CGI 的结合体,但是其运行效率却要比 CGI 高。ASP 与 CGI 最大的不同在于对象和组件的使用,ASP 除了内置的 Request、Response、Server、Session、Application 及 ObjectContext 等基本对象外,还允许用户以外挂的方式使用 ActiveX 控件。当然,ASP 本身也提供了多个 ActiveX 控件供使用,这些组件包括广告回转组件、文件存取组件、文件连接组件及数据库存取组件等,这些大量扩充且可以重复使用的组件使得 ASP 的功能远远强于 CGI。

3. PHP

PHP (Hypertext Preprocessor, 超文本预处理器) 是一种 HTML 内嵌式的语言 (类似于 ASP)。PHP 秉承 Linux 的 GNU 风格,借助于源代码公开,成为目前广泛应用的动态网页开发技术之一。PHP 独特的语法混合了 C、Java、Perl 及 PHP 式的新语法,它执行动态网页的速度也比 CGI 快。从性能、开发及维护时间上看,PHP 和 ASP 是并驾齐驱的,它们都有不错的表现。

4. JSP

JSP (Java Server Pages, Java 服务器页面) 是 Sun 公司推出的网站开发技术,是将纯 Java 代码嵌入 HTML 中实现动态功能的一项技术。目前,JSP 已经成为 ASP 的有力竞争者。

JSP 与 ASP 技术非常相似,两者都是在 HTML 代码中嵌入某种脚本,并由语言引擎解释执行程序代码,它们都是面向服务器的技术,客户端浏览器不需要任何附加软件的支持。

两者最明显的区别在于 ASP 使用的编程语言是 VBScript 之类的脚本程序,而 JSP 使用的是 Java。此外,ASP 中的 VBScript 代码被 ASP 引擎解释执行,而 JSP 中的脚本在第一次执行时被编译成 Servlet 并由 Java 虚拟机执行,这是 ASP 与 JSP 本质的区别。

5. ASP.NET

作为微软 .NET 框架中重要的组成部分,ASP.NET 越来越多地受到开发人员的关注。传统的 ASP 技术中 ASP 程序和网页的 HTML 标记混合在一起,造成了网页美工设计人员和程序设计人员在相互配合过程中会出现诸多的不便;此外,ASP 页面的脚本语言是解释执行的,其执行速度较慢。为了克服 ASP 以上的种种限制,微软推出了 ASP.NET。

ASP.NET 不是 ASP 的一个简单升级，它提供了一个全新且功能强大的服务器控件结构。从表面上看，ASP.NET 和 ASP 是相近的，但从本质上看是完全不同的。ASP.NET 几乎全是基于组件和模块化，每一个页面、对象和 HTML 元素都是一个运行的组件对象。在开发语言上，ASP.NET 抛弃了 VBScript 和 JScript，而使用 .NET 框架所支持的 VB.NET, C# 等语言作为其开发语言，这些语言生成的网页在后台被转换成了类并编译成了一个 DLL（动态链接库）。由于 ASP.NET 是编译执行的，所以它比传统的 ASP 执行效率更高。

鉴于 ASP 技术的使用较为广泛，其技术发展比较成熟，相关资料较多，本书将主要介绍 ASP 技术。由于 ASP 易学、易用，在学习好 ASP 技术后，触类旁通、举一反三，再去学习其他的动态网页技术就会比较容易了。

1.2 ASP 概述

ASP（Active Server Pages，活动服务器网页）是 Microsoft 公司推出的一项动态网页开发技术。ASP 是一种服务器端脚本编写环境，可以创建和运行动态、交互且高效的 Web 服务器应用程序。

1.2.1 ASP 的特点

ASP 具有以下几个重要的特点：

（1）在 ASP 页面中可以包含文本、HTML 标记、服务器端脚本和客户端脚本命令及 ActiveX 组件。Web 服务器只执行 ASP 页面中的服务器脚本，页面中的其他内容被服务器原封不动地发送给客户机浏览器。

（2）ASP 中可以有多种脚本语言，包括 VBScript 和 JScript。在安装了相应的脚本引擎后，还可以使用其他脚本语言。

（3）ASP 提供了一些内置对象，使用这些内置对象可以增强 ASP 的功能。例如，实现客户机浏览器与 Web 服务器的交互，在网页间传递参数等功能。

（4）ASP 可以使用内置的 ActiveX 组件完成许多重要的功能。例如，借助 ADO 对象，可以轻松地完成对数据库的操作。当然，也可以使用其他第三方提供的组件来完成特定的功能。

（5）ASP 具有一定的安全性。由于 ASP 页面是在服务器端运行的，送到客户机浏览器的是 ASP 的执行结果所生成的 HTML 页面，用户只能得到 HTML 代码而无法获取 ASP 页面源代码。

（6）ASP 是一种解释性语言，服务器只要在使用时对其进行解释执行即可。

1.2.2 ASP 文件的基本结构

ASP 文件是以 .asp 为扩展名的文本文件，可以使用任何一种文本编辑器（如 Windows 中的记事本、写字板）创建，也可以使用那些带有 ASP 增强功能的编辑器（如 FrontPage、Dreamweaver 等）来提高工作效率。

在 ASP 文件中通常包含以下 3 部分的内容：

- （1）HTML 标记。
- （2）脚本命令。