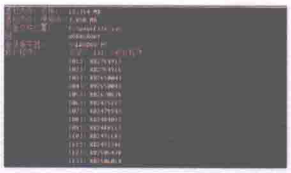
关于本书

知己知彼，才可百战不殆；全书会对每一个入侵步骤做详细地分析，以推断入侵者每一个入侵步骤的目的以及所要完成的任务，并对入侵过程中常见的问题作必要的说明与解答，旨在帮助网络安全维护人员真正从实践角度制定防范计划。

本书的主要目的是向读者介绍当前网络安全中黑客攻防技术的思考方法，以期从根本上保障Web安全。

黑客攻防



Web安全实战详解

Hacking and Defence——the Practice Detailed of Web Security

精准定位
本书写作目标定位于当前网络安全的主要"战场"：Web安全

真实环境
从防范角度描述一个真实的入侵案例，给出完善的安全方案

丰富案例
作者精炼筛选大量真实攻防案例，步骤详细，讲解翔实到位

在线交流
作者组建在线QQ技术群以及微信公众平台，为读者在线答疑

赵 彬 编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

黑客攻防

Web安全实战详解

Hacking and Defence——the Practice Detailed of Web Security

赵彬 编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书用 3 篇共计 9 章的篇幅向读者介绍了当前网络安全之中重要的领域：Web 安全，作者通过网络安全基础知识的精练讲述，入侵环境的真实模拟，防范技巧的实践总结，向读者展示了在网络实践环境中如何做到知己知彼，有效地防范黑客的攻击。

本书适合网络安全从业人员尤其是网站安全维护人员使用，同时本书中的安全防范技巧对普通网络用户用于保护自己的数据安全也非常实用。

图书在版编目（CIP）数据

黑客攻防 ：Web 安全实战详解 / 赵彬编著. — 北京：中国铁道出版社，2014.7

ISBN 978-7-113-18270-0

Ⅰ.①黑… Ⅱ. ①赵… Ⅲ. ①计算机网络－安全技术 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字（2014）第 064062 号

书　　名：黑客攻防：Web 安全实战详解
作　　者：赵　彬　编著

责任编辑：荆　波　　**读者热线电话**：010-63560056
特邀编辑：杜长芸　　**封面设计**：多宝格・付　巍
责任印制：赵星辰

出版发行：中国铁道出版社（北京市西城区右安门西街 8 号　　邮政编码：100054）
印　　刷：北京鑫正大印刷有限公司
版　　次：2014 年 7 月第 1 版　　2014 年 7 月第 1 次印刷
开　　本：787mm×1092mm　1/16　　**印张**：23.5　**字数**：563 千
书　　号：ISBN 978-7-113-18270-0
定　　价：49.80 元

前　言

本书主要针对网络安全从业人员，尤其是网络（站）管理员；书中更深入、细致地剖析黑客技术（尤其是 Web 安全技术），系统性强，以期满足那些已有一定技术基础的读者的需要。此外，值得一提的是，笔者始终以“授之以鱼，不如授之以渔”为基本出发点来展开本书的内容。也就是说，本书的主要目的是向读者介绍黑客攻防技术的思考方法，而不是单纯地介绍某个工具的使用方法。总之，本书是一本介绍为什么，而不是单单介绍怎么做的一本网络安全与黑客攻防技术图书，这一点是本书区别于其他黑客类书籍的根本特征。

为什么写作本书

不容乐观的是，有一部分人歪曲了黑客的本质，被不良动机所驱使，进行各种入侵活动，威胁网络的健康发展。对于我国来说，形势尤为严峻。我国信息化建设迟于美国等发达国家，信息安全技术水平也相对落后，在几次跨国的黑客大战中，国内网站的弱口令、漏洞比比皆是，这种现状实在令人担忧，值得我们深思和反省，从中也可以看出国内传统的计算机、网络教学远远没有满足实际的需要。可能出于安全等因素的考虑，传统教学往往只教授简单的应用，避开了一些敏感的技术。设想一下，如果一个网站的管理员只学会架构网站，却不关心如何入侵自己的网站，那么他如何对自己网站的缺陷了如指掌？如何能够及时地获知最新漏洞而提前做好抵御？如果以上都做不到，那就更不要谈日常的系统更新、维护和打补丁了。然而，国内精通入侵的网管又有多少呢？长期以来，国内网管的潜意识里都认为“入侵”是个不光彩的勾当，甚至嗤之以鼻。随着信息化程度越来越高，信息技术与生活的联系越来越紧密，可以上网的电子设备逐年增加，电脑、PDA、手机，甚至家电。可以想象 10 年后，如果不了解入侵者的手段来采取必要的防御措施，将要被入侵的设备不会仅仅限于电脑，也许还包括你的手机、家电、汽车，等等。因此，在信息技术如此发达，沟通方式日益丰富和复杂的今天，我们不仅要学会如何正确使用网络，而且还需要学会如何防御自己的网络被他人入侵。

出于以上原因，笔者通过多年的研究与实践，系统地总结了目前广为使用的入侵、防御技术，并针对广大网管以及对网络感兴趣的爱好者编写了本书。希望大家能够从多个角度来了解网络安全技术，至少做到知己知彼。

本书主要内容

本书深入浅出，先从网络基础知识讲起，深入剖析入侵过程为主线来展开全书内容，向读者介绍入侵者如何实现信息的收集，如何通过获取的信息打开目标服务器的切入点，如何实现入侵即远程连接，入侵后如何执行各种任务，如何留下后门以便再次进入系统，以及入侵者如何清除系统日

志防止目标服务器发现入侵痕迹。此外，书中还详细地介绍了入侵者是如何实现从信息扫描到入侵过程中的隐身保护，如何逃避被他人发现。全书会对每一个入侵步骤做详细的分析，以推断入侵者在每一入侵步骤的目的以及所要完成的任务，并对入侵过程中常见的问题作必要的说明与解答，此外，还会对几种常见的入侵手段进行比较与分析。

本书按照难易程度分为“基础篇”、“实战篇”和“提高篇”，3 篇共 9 章，每章的主要内容如下。

第 1 章“网络基础”：深入浅出介绍网络相关的基础知识，其中包括什么是网站，什么是网络，什么是网络程序等。

第 2 章“信息集与社会工程学”：介绍网络安全入侵的第一步，也是非常重要的一步——信息搜集，从技术的层面和社会工程学的层面介绍了黑客惯用的信息搜集手法。

第 3 章“一次完整的入侵”：通过一个完整的入侵实例来介绍入侵的一般手法，使读者对入侵手法有个初步的认识。

第 4 章“基于 Web 的入侵”：系统地介绍了 Web 入侵的基本手法。目前 Web 入侵也是一个最常用的手段。

第 5 章“基于提权的入侵”：介绍了如何基于用户名+密码认证方式进行提权，从而入侵远程主机。

第 6 章“基于网马和木马的入侵”：介绍了入侵者如何通过种植木马程序来实现入侵的目的。

第 7 章“基于内网的入侵”：介绍了入侵者通过局域网、内网进行入侵。

第 8 章“留后门与清脚印”：介绍了入侵成功后，入侵者如何抹去入侵痕迹并留下后门以便再次入侵。

第 9 章“BAT 编程”：介绍了 BAT 编程的一般方法。在入侵过程中，入侵者经常编写一些 BAT 程序来简化烦琐的入侵过程。

笔者将提供 QQ 群和微信公众平台供广大读者和作者交流。

QQ 群号：黑客攻防丛书读者会 27300920

微信公众平台：网路安全集训营

需要声明的是，**本书的目的绝不是为那些怀有不良动机的人提供支持，也不承担因为技术被滥用所产生的连带责任；本书的目的在于最大限度地唤起大家的网络安全防护意识，请勿将本书中所讲技术用于任何违法活动，否则后果自负，切记！**

限于编者水平有限，加之时间仓促，书中错漏之处在所难免，敬请广大读者批评指正。

编　者

2014 年 5 月

目　录

基　础　篇

第 1 章　网络基础 2
1.1　什么是网站 2
1.1.1　网站与计算机 2
1.1.2　访问一个网站 2
1.1.3　浏览和下载内容 3
1.2　什么是网络 3
1.2.1　计算机网络 3
1.2.2　OSI/RM 模型 4
1.2.3　IP 协议和 TCP/IP 模型 4
1.2.4　端口 5
1.2.5　Web 服务协议 6
1.3　什么是网站程序 6
1.3.1　静态网页与动态网页 6
1.3.2　网页语言 7
1.3.3　URL 传值 9
1.3.4　查看源代码与审查元素 9
1.4　数据库 11
1.4.1　数据库的定义与类型 11
1.4.2　常见的数据库 11
1.4.3　结构化查询语言 12
1.4.4　数据库在网页中的使用 13
1.5　什么是服务器 15
1.5.1　服务器的概念 15
1.5.2　服务器系统与服务 15
1.5.3　安装与配置 Web 服务器 15
1.6　小结 18
第 2 章　信息搜集与社会工程学 19
2.1　网站信息搜集 19
2.1.1　基础信息 19
2.1.2　whois 查询 21
2.1.3　备案信息 22

2.1.4 精通站长工具 23
2.1.5 拓扑探测 25
2.2 端口扫描 26
2.2.1 基础知识 26
2.2.2 端口扫描原理 27
2.2.3 实战端口扫描 28
2.3 综合扫描 29
2.3.1 Web 目录扫描 30
2.3.2 Web 漏洞扫描之 safe3wvs 33
2.3.3 Web 漏洞扫描之 AppScan 34
2.3.4 系统级漏洞扫描之 X-Scan 40
2.3.5 系统级漏洞扫描之 Nessus 44
2.3.6 在线扫描工具 SCANV 50
2.3.7 其他著名漏洞扫描工具简介 54
2.4 Googlehack 57
2.4.1 搜索引擎基本语法 57
2.4.2 搜索网站后台 58
2.4.3 搜索网站注入点 59
2.4.4 搜索网站目录 60
2.4.5 漏洞挖掘鸡 62
2.5 社会工程学 63
2.5.1 浅谈社会工程学 63
2.5.2 账号密码的安全性 64
2.5.3 社交网络的隐私安全 65
2.5.4 认识网络钓鱼攻击 66
2.6 小结 68

实 战 篇

第 3 章 一次完整的入侵 70
3.1 安装虚拟机 70
3.2 搭建服务器及网站 79
3.3 一次完整的入侵演示 85
3.4 小结 95
第 4 章 基于 Web 的入侵 96
4.1 Web 欺骗攻击 96
4.1.1 网络钓鱼 96

4.1.2 基于页面的 Web 欺骗 103
4.1.3 基于程序的 Web 欺骗 108
4.2 SQL 注入 114
4.2.1 测试环境的搭建 115
4.2.2 一个简单的实例 119
4.2.3 用浏览器直接提交数据 127
4.2.4 注入漏洞的利用 129
4.2.5 注入漏洞的高级利用 133
4.2.6 对 Very-Zone SQL 注入漏洞的利用 141
4.2.7 对动易商城 2006 SQL 注入漏洞的利用 145
4.2.8 使用工具进行 SQL 注入 151
4.2.9 对 SQL 注入漏洞的防御 157
4.3 跨站脚本攻击 160
4.3.1 跨站的来源 160
4.3.2 简单留言本的跨站漏洞 161
4.3.3 跨站漏洞的利用 165
4.3.4 未雨绸缪——对跨站漏洞的预防和防御 174
4.4 Web 后门及加密隐藏 175
4.4.1 什么是 Web 后门 176
4.4.2 Web 后门免杀 177
4.4.3 Web 后门的隐藏 178
4.5 Web 权限提升 184
4.5.1 系统漏洞提权 185
4.5.2 第三方软件权限提权 186
4.5.3 配置不当提升系统权限（陷阱式提权） 192
第 5 章 基于提权的入侵 200
5.1 Windows 权限 200
5.1.1 认识 Windows 权限 200
5.1.2 Windows 用户组及其权限 203
5.1.3 webshell 权限 205
5.2 服务器漏洞提权 206
5.2.1 webshell 提权流程 206
5.2.2 服务器本地提权漏洞 212
5.3 第三方软件提权 218
5.3.1 MySQL root 提权 218
5.3.2 MS-SQL sa 提权 220

5.3.3 其他第三方提权简介 222
5.4 3389 远程连接 224
5.5 lcx 端口转发 226
第 6 章 基于网马和木马的入侵 229
6.1 网马 229
6.1.1 认识网马 230
6.1.2 木马免杀 233
6.1.3 网马隐藏 237
6.2 木马和后门 237
6.2.1 赤兔马 237
6.2.2 木马免杀 244
6.2.3 黑客的最爱——Rootkit 257
第 7 章 基于内网的入侵 264
7.1 内网基础知识 264
7.1.1 什么是内网 264
7.1.2 路由器的搭建 266
7.1.3 网络拓扑结构 277
7.1.4 旁注和 C 端认识 281
7.1.5 域的认识和搭建 284
7.2 内网信息刺探 298
7.2.1 获取主机网络信息 298
7.2.2 获取主机用户密码 301
7.3 ARP 攻击 308

提 高 篇

第 8 章 留后门与清脚印 318
8.1 账号后门 318
8.1.1 手工克隆账号 319
8.1.2 命令行方式下制作后门账号 327
8.1.3 克隆账号工具 331
8.1.4 常见问题与解答 335
8.2 漏洞后门 335
8.2.1 制造 Unicode 漏洞 335
8.2.2 制造.idq 漏洞 337
8.3 木马后门 338
8.3.1 wollf 338

8.3.2 Winshell 与 WinEggDrop 344
8.3.3 SQL 后门 346
8.4 清除日志 348
8.4.1 手工清除日志 348
8.4.2 通过工具清除事件日志 349
8.4.3 清除 WWW 和 FTP 日志 351
8.5 小结 353
第 9 章 BAT 编程 354
9.1 批处理命令简介 354
9.2 在批处理文件中使用参数与组合命令 359
9.2.1 在批处理文件中使用参数 359
9.2.2 组合命令 360
9.3 管道命令 361
9.4 综合利用的实例 364
9.4.1 系统加固 364
9.4.2 删除日志 364
9.5 小结 365

基 础 篇

本篇中通两个章节的内容，介绍了网络安全学习中必须掌握的基础知识；第 1 章详细阐述了网站、网站程序、数据库以及服务器等的概念和基本操作；第 2 章从技术层面和社会工程学层面介绍了黑客惯用的信息搜集手法。

第 1 章　网络基础

黑客技术与计算机领域其他技术的一个很大区别是黑客技术的非公开化。大家很少看到教科书或媒体对黑客技术进行大范围公开宣传，以致很多人认为黑客技术很神秘，甚至认为黑客技术很邪恶。那么，作为开篇，我们从网络基础知识开始，逐渐揭开黑客技术的神秘面纱，走进黑客技术“矛”与“盾”的神秘世界。

1.1　什么是网站

日常生活中，我们经常浏览各种网站，这些网站内容丰富，功能不一，传递的信息满足了人们的各种需要。但是，网站在网络中究竟是什么，它存在于网络上还是别人的计算机上？而网络究竟由什么组成，如何实现，是什么结构呢？

1.1.1　网站与计算机

网站置于服务器中，而服务器则是指连接在网络中的一台计算机。当我们浏览网站时，实际上就是我们用个人计算机通过网络访问在网络上的一台计算机中网站应用程序的过程。

1.1.2　访问一个网站

打开 IE 浏览器，在地址栏中输入 http://www.microsoft.com/en-us/default.aspx 来访问微软的官方站点。如图 1-1 所示，我们已经成功地访问了微软网站。其中，如图 1-2 所示，我们访问网站的时候输入的那串字符，就是我们常说的“网址”。

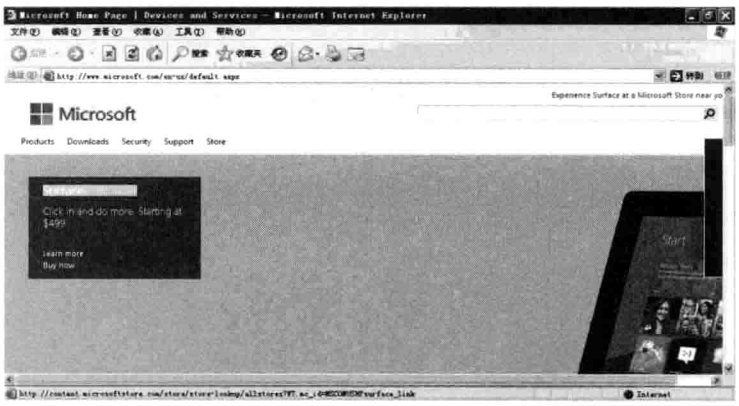


图 1-1

图 1-2

每个网址对应一个或多个 IP 地址，该 IP 地址指向了存放网站的服务器。因此，我们可以通过输入网址和输入 IP 地址两种方式来访问此网站。但是，即使输入网址最后还是需要解析成 IP 地址来访问网站服务器，我们之所以经常用网址而不用 IP 地址，是因为相比较而言，网址更容易被我们记住。

1.1.3　浏览和下载内容

网站到底是怎么一回事儿呢？我们为什么可以浏览和下载网站上的内容？

如图 1-3 所示，我们在网站上一个 Logo 图片的位置单击右键→属性，会出现“属性”对话框（见图 1-4）。这意味着我们浏览一个网站的过程，实际上就是访问网络上一台服务器上的文件。

图 1-3

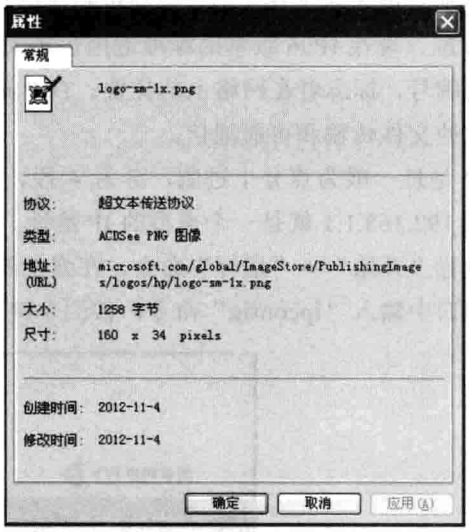


图 1-4

1.2　什么是网络

1.2.1　计算机网络

计算机网络是指通过通信线路与通信设备与远方终端进行的连接。简单来说，由多台计算机或其他网络设备通过传输介质和网络协议连接在一起组成。计算机网络按不同的角度可以进行多种分类。常见的按物理拓扑结构可分为星形、环形、总线型、网状和树形及混合型等；按网络带宽可分为宽带网和窄带网；按信息的交换方式可分为电路、报文和分组交换等；而最常

见的按照网络作用的地理覆盖范围可分为局域网（LAN）、城域网（MAN）和广域网（WAN）。因特网（Internet）是世界上最大的广域网。

1.2.2 OSI/RM 模型

国际标准化组织（International Standard Organization，ISO）在 1978 年提出了“开放系统互联参考模型”，即著名的 OSI/RM 模型（Open System Interconnection/Reference Model，OSI/RM）。它将计算机网络体系结构的通信协议划分为七层，自下而上依次为：物理层（Physics Layer）、数据链路层（Data Link Layer）、网络层（Network Layer）、传输层（Transport Layer）、会话层（Session Layer）、表示层（Presentation Layer）、应用层（Application Layer）。

1.2.3 IP 协议和 TCP/IP 模型

IP 协议就是定义路由器、交换机和网络结点之间通信的一种标准方法。我们普遍使用的是 IPv4 标准，现在 IPv6 版本的标准适用也越来越多。每一个上网用户都会被分配一个 IP 地址，就像门牌号，标志着在网络上的位置。TCP 是目前使用最多的传输层协议，它完成了因特网上大多数的文件传输和可靠通信。

IP 地址一般为点分十进制，分为 4 段，每段的数字范围为 0～255，段与段之间用句点分隔，如 192.168.1.1 就是一个典型的 IP 地址。

执行“开始”→“运行”命令，在弹出的对话框中输入“cmd”，单击“确定”按钮，在打开的窗口中输入“ipconfig”命令，按回车键，即可查看本机 IP 地址，如图 1-5～图 1-7 所示。

图 1-5

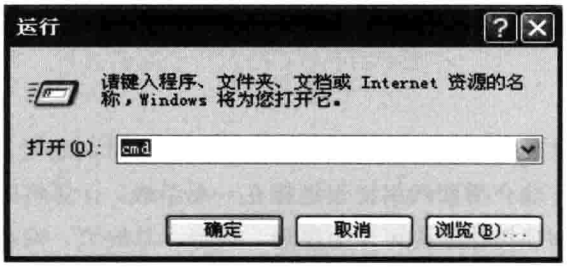


图 1-6

图 1-7

1.2.4　端口

这里所说的端口并不是并行端口和串行端口等硬件端口，也非软件结构和数据结构中的软件端口，而是指“协议端口”。

大家都知道 IP 是每个连到网络上的计算机的地址，就像门牌号一样。倘若把一台计算机比作一间屋子，IP 是门牌号，而端口就是出入这间屋子的大门。一台计算机的端口可达 65 536（即 2^16）之多，范围以从 0 到 65 535 的整数来标记。

不同的端口对应着不同的服务，常用端口如下。

- 21 端口：主要用于 FTP（File Transfer Protocol，文件传输协议）服务。
- 23 端口：主要用于 Telnet（远程登录）服务，是 Internet 上普遍采用的登录和仿真程序。
- 25 端口：为 SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）服务器所开放，主要用于发送邮件，如今绝大多数邮件服务器都使用该协议。
- 80 端口：是为 HTTP（Hyper Text Transport Protocol，超文本传输协议）开放，这是上网冲浪使用最多的协议之一，主要用于在 WWW（World Wide Web，万维网）服务上传输信息的协议。
- 109、110 端口：109 端口是为 POP2（Post Office Protocol Version 2，邮件协议 2）服务开放的，110 端口是为 POP3（邮件协议 3）服务开放的，POP2、POP3 主要用于接收邮件。
- 135 端口：主要用于使用 RPC（Remote Procedure Call，远程过程调用）协议并提供 DCOM（分布式组件对象模型）服务。
- 137 端口：主要用于“NetBIOS Name Service”（NetBIOS，名称服务）。
- 139 端口：是为“NetBIOS Session Service”提供的，主要用于提供 Windows 文件和打印机共享以及 UNIX 中的 Samba 服务。
- 161 端口：用于“Simple Network Management Protocol”（SNMP，简单网络管理协议）。
- 3389 端口：是最常见的远程桌面服务端口。
- 4000 端口：用于 QQ 聊天工具，主要是为 QQ 客户端开放的端口，QQ 服务端使用的是 8000 端口。

- 5632 端口：是为远程控制软件 pcAnywhere 所开启的端口。
- 8080 端口：同 80 端口，用于 WWW 代理服务，可以实现网页浏览。

执行“菜单”→“运行”命令，在弹出的对话框中输入“cmd”，单击“确定”按钮，在打开的 DOS 界面窗口中输入“netstat -on”命令，按回车键即可查看该计算机本地开放的端口，如图 1-8 所示。

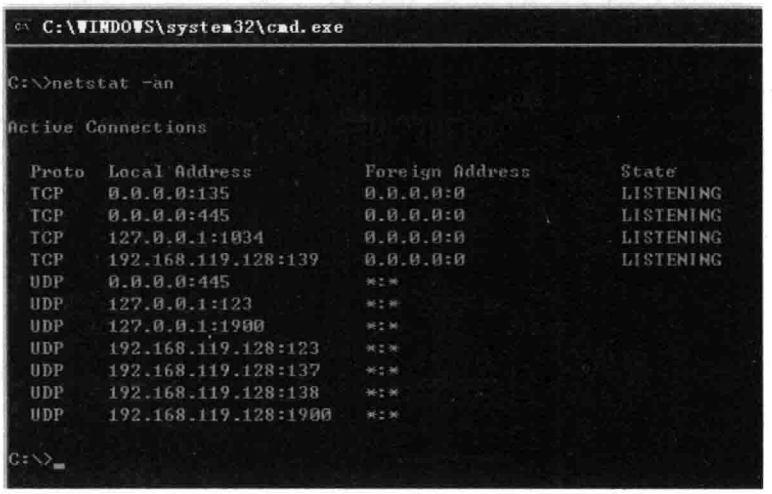


图 1-8

1.2.5 Web 服务协议

通过以上介绍我们了解到，访问一个网站的过程实质上就是通过 IP 地址找到对方计算机，然后通过对方计算机开放的相应端口（通常为 80 端口）来访问其网站内容。而网页内容的传输过程也必须按照一定的协议来进行，互联网的秩序才可以有条不紊地保持下去。

Web 服务支持 3 种协议来与用户交流数据。这 3 种协议分别是：HTTP-GET、HTTP-POST 和 SOAP。其中，HTTP-GET 和 HTTP-POST 是最简单的，一般用来与 Web 服务进行交互的协议；SOAP 是 XML Web Service 最常用到的连接协议。与 HTTP 相比，SOAP 显得更为复杂，但却拥有更强的接受能力。

1.3 什么是网站程序

1.3.1 静态网页与动态网页

我们知道，一个网站是由一张张网页组成的，而网页又分为静态网页与动态网页。最早的网页仅仅由静态文档构成，用户浏览时只能读取网页内容。随着网络的发展，人们可以向 HTML 文档中嵌入程序或添加动态脚本，从而构成可以与用户进行交互的动态网页，其功能和内容与

传统的静态网页相比更丰富，更新颖。

- 静态网页：通常就是纯 HTML 格式的网页，早期的网站一般由静态网页构成。其文档扩展名为.htm、.html、.shtml 等。虽然在 HTML 格式的网页中也可以出现各种动态的效果，如插入 gif 格式的图片或者制作 Flash，甚至可以用 html 标签实现滚动字幕的效果，但这些“动态”仅限于视觉上，和真正的动态网页有很大的区别。
- 动态网页：与静态网页形成对比，动态网页不是指视觉上的“动态”，其动态主要体现在“交互性”上，往往同一个网页文件能根据不同的请求和访问时间显示不同的内容。动态网页能与后台数据库进行交互，数据传递，也就是说，其内容可以存储在数据库中，这样大大方便了调用和管理以及维护。

动态网页与静态网页最本质的区别，就是网页制作的语言的不同，动态网页以超文本标记语言 HTML 为基础，结合动态网页技术组成，一般以.asp、.aspx、.php、.jsp、perl、cgi 等为扩展名，并且在动态网页网址中常常出现一个标志性的符号“？”，该符号的作用，我们在后文会提到。采用动态网页技术的网站可以实现更多的功能，如用户注册、用户登录、在线调查、用户管理、订单管理等。但是，在功能变多的同时，程序也变得更加复杂与庞大，由于程序员的疏忽，往往会出现许多漏洞。

1.3.2　网页语言

静态网页是由超文本标记语言组成的，而动态网页是从超文本标记语言为基础的，所以我们有必要了解一下这个超文本标记语言（HTML）。

HTML 是用来描述网页的一种语言。它不是一种编程语言，而是一种标记语言（markup language）。标记语言是一套标记标签，也就是说 HTML 使用标记标签来描述网页。HTML 标签是由简括号包围的关键词，如<html>。HTML 标签通常是成对出现的，如和。通常一对标签中，第一个标签是开始标签，第二个标签是结束标签，或称为开放标签和闭合标签。

实际上，HTML 文档就是网页，HTML 文档包含 HTML 标签和纯文本。Web 浏览器的作用是读取 HTML 文档，并以网页的形式显示出它们。浏览器不会显示 HTML 标签，只是通过识别标签来解释网页的内容。下面我们通过一个 html 网页的源代码来初步认识 html 语言。

```
<html>
<body>
<title>这是一个 Html 文档（网页）</title>
<p>这是一个段落</p>
</body>
</html>
```

<html>与</html>之间涵括的是网页的主体，其中的文本都用于描述网页。而<body>与</body>之间是可显示的文本，其中的内容就是我们要体现在网页上的内容（并非显示）。 与 标记一个段落，其中的内容会以段落的形式显示在网页上。静态网页就是用一对对标签