宝典丛书 200万

网络安全与黑客攻防

（第2版）

宝典

本书包括根据实战经验精心改编的实例，充分考虑读者的理解水平，使其能够根据自身的知识水平有针对性地学习，思路变得更加开拓。

本书知识面开阔，有基础性知识，也有深入的理论探讨，满足不同程度读者的阅读需求。

本书使用大量的新知识，如Metasploit、Nessus、UTM、EnCase、网络钓鱼、流氓软件和NetStumbler等，使本书与同类书中陈旧的技术内容形成鲜明的对比，阅读价值得到极大提升。

李俊民　郭丽艳　等编著

電子工業出版社
Publishing House of Electronics Industry
http://www.phei.com.cn

宝 典 丛 书

网络安全与黑客攻防宝典

（第2版）

李俊民　郭丽艳　等编著

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

内 容 简 介

本书由浅入深、循序渐进地介绍了计算机网络安全的知识体系。全书共分 21 章，内容涵盖网络的基础知识、黑客初步、操作系统漏洞与应用软件漏洞的攻防、BBS 与 Blog 的漏洞分析、信息收集、扫描目标、渗透测试、网络设备的攻击与防范、木马分析、病毒分析、网络脚本攻防、SQL 注入攻防、防火墙技术、入侵检测技术、计算机取证、无线网络安全等内容。本书最大的特色在于知识全面、实例丰富，每一节的例子都经过精挑细选，具有很强的针对性，读者可以通过亲手实践进而掌握安全防护的基本要领和技巧。

本书适合初、中级用户学习网络安全知识时使用，同时也可作为高级安全工程师的参考资料。

图书在版编目（CIP）数据

网络安全与黑客攻防宝典 / 李俊民，郭丽艳等编著.—2 版.—北京：电子工业出版社，2010.3
（宝典丛书）
ISBN 978-7-121-10081-9

Ⅰ. 网… Ⅱ.①李…②郭… Ⅲ.计算机网络－安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2009）第 229544 号

责任编辑：于 兰
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市鑫金马印装有限公司
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：787×1092　1/16　　印张：50.75　　字数：1445 千字
印　　次：2010 年 3 月第 1 次印刷
定　　价：89.00 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。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件到 dbqq@phei.com.cn。

服务热线：（010）88258888。

第 2 版说明

本书第一版出版后受到了广大读者的青睐，曾多次印刷。随着技术的不断发展，黑客的攻击手段也越来越多，网络安全面临着越来越严峻的考验，人们不得不对网络安全更加重视。由于本书第一版中的一些内容和技术有所过时，所讲述的一些工具和技术都有了新的发展，也出现了一些新的工具和攻防手段，所以有必要对本书第一版内容进行升级，以适应当前网络安全的技术需求。

第二版在第一版内容的基础上对所有旧版本的工具进行了更新，并且添加了 7 章新的内容，并对第一版中存在的一些遗漏进行了校正和增补。

本书新增内容主要有如下几个方面：

- 计算机病毒和木马的防范方法
- 如何摆脱脚本攻击
- 网络封锁和代理突破
- 计算机操作系统的攻防技术及软件和文件的加密技术
- SQL 注入攻防技术
- 欺骗攻击技术实施攻击的原理及安全防范
- 后门技术与痕迹清理技术

前　言

在当今的网络时代，黑客、病毒让人们谈虎色变，那么到底什么是黑客，他们如何工作，病毒到底是什么，病毒的出现又会对人们的生活造成什么样的影响？本书将给出这些问题的答案。

计算机网络安全是现今网络的主旋律，关于网络安全的话题在媒体上随处可见。随着黑客工具的日益“傻瓜”化，黑客已经被剥离了神秘的外衣。但是计算机安全、网络安全知识的普及仍然是一个严峻的问题，为了解决这个问题，本书以普及安全知识为己任，帮助用户深入了解网络安全的方方面面，如深入分析黑客入侵计算机的全过程，模仿黑客入侵计算机并提升远程计算机的权限进而达到控制的目的，剖析病毒和木马的来龙去脉，预测入侵检测的技术发展及趋势，此外，神秘的计算机取证技术和热点的无线网络安全问题都将在本书中呈现。

本书依照读者的学习规律，首先从了解网络安全的基础知识讲起，介绍基本概念和基本观点，在读者掌握了这些基本知识的基础上，再介绍历史上著名的黑客人物及历史事件，以立体的角度、有趣的故事情节为依托，严格遵循由浅入深、循序渐进的原则。本书以计算机网络安全知识的层次结构为主线将各种工具、命令和理论知识交织编排在一起，使读者可以深入学习任何一章的内容。

本书在内容编排和目录组织上都十分讲究，章节之间既可相互呼应也可各自成章。比如在第 1 章熟悉了网络的基础知识以后，立刻引入一些著名的黑客人物的经历，以一个实例告诉读者这些知识的重要性，让读者在茶余饭后的闲谈中即可快速入门。同时，每章之间又相互独立，如果读者希望直接了解病毒的相关知识，可快速查阅第 9 章和第 10 章。第 9 章对木马进行了深入的分析，第 10 章按照病毒的机制对病毒进行了深入的剖析。

本书特色

和其他书籍相比，本书具有以下特点：

- **内容丰富，实例经典。**
  在学习计算机网络安全知识时，经常遇到两种情况，一是单纯地讲理论而对知识实践只字不提；另外就是纯粹讲解实战而对涉及的理论不予理会。本书则不同，本书追求理论与实践的结合，使用浅显的语言尽可能地通过精心设计的经典实例，将计算机网络安全的基本理论和实践技巧融入到范例当中，全面覆盖计算机网络安全的各个角落。
- **实战众多，内容充实。**
  作者在讲解每一个知识点之后，都要安排尽可能多的实例。这些实例都是根据实战经验改编，充分考虑了读者的理解水平，并且实战的每一步都介绍得非常详细，读者能够根据自身的知识水平有针对性地学习，使思路变得更加开拓。

- **讲解通俗，步骤详细。**
  每个实例的演练步骤都以通俗易懂的语言阐述，并穿插说明文字，还附加了详细的插图作为演练的参考。
- **知识面开阔，重点突出。**
  本书涉及的内容众多，有基础知识，也有深入的理论探讨。为了说明某一个知识点，在前面使用了一些基础知识作为铺垫，这些知识既可作为了解的必要步骤，也可作为参考知识供读者查阅。
- **新知识多，讲解全面。**
  在本书中介绍了大量的新知识，如 Metasploit、Nessus、UTM、EnCase、网络钓鱼、流氓软件和 NetStumbler 等。这些新知识的介绍充实了本书的内容，也使得本书与同类书中陈旧的技术内容形成了鲜明的差别。本书不仅介绍了新知识，而且针对这些知识进行实战演练，帮助读者快速了解新内容。
- **实例鲜活，应用软件可随时获得。**
  虽然本书中使用了大量软件，但是这些软件基本上都是免费软件，读者可以从网络上随时下载进行练习，这就避免了读者只能阅读，不能实战的尴尬。
- **兼顾各种水平的读者。**
  虽然本书面向基础读者，但是本书中也介绍了很多理论知识，这些内容为高级读者可以提供进一步参考。

本书内容

本书包括以下内容：

第 1 章 首先介绍网络的基本体系构成、网络的工作原理、黑客的基本知识、常用的端口知识，以及一般性的安全防范知识。

第 2 章 切入正题，介绍黑客的一些情况，如历史上的著名黑客及其参与的事件、著名的黑客组织、黑客通常使用的入侵手法和这些手法的防范方法等。

第 3 章 以操作系统常见的漏洞为主题，介绍如何利用这些漏洞入侵远程计算机的过程，并给出了防范方法。另外，还介绍了服务器软件的一些漏洞及其解决方法。

第 4 章 继续第 3 章，重点分析 BBS 系统和 Blog 系统的一些问题，如提升权限、Cookies 问题及数据库暴库的问题。

第 5 章 帮助读者了解高级黑客搜集信息的工具及方法，如使用 Google 搜集网站信息、DNS 查询和追踪路由等知识。

第 6 章 主要介绍各种扫描技术及技巧，如 SYN 扫描、圣诞树扫描、FIN 扫描、空扫描、UDP 扫描等，还介绍了操作系统协议栈指纹识别技术。这一章使用了各种著名的扫描器，并给出了实战分析。

第 7 章 介绍黑客入侵的高级知识及渗透测试。其中重点介绍了一些渗透测试的基础知识和测试过程中涉及的技术问题，如分析缓冲区溢出问题及各种溢出知识，还介绍了数据库及 Web 渗

透的基本技术，并在最后演示了一种在国外非常流行的测试工具平台 Metasploit 的使用方法。

第 8 章 介绍网络设备的基本知识，如路由器和交换机的工作原理，以及一些常用的网络设备攻击方法，如使用 SNMP 对路由器入侵及 TFTP 的使用方法。

第 9 章 从各个角度对木马进行了深入剖析。其中涉及木马的基本概念、木马常用攻击手段、木马程序的隐藏技术、木马攻击的防范与清除；介绍一些典型木马，如灰鸽子、冰河、RAdmin 的基本知识；还介绍了使用冰刃检查木马进程及 Ethereal 防范木马的一些方法和技巧。

第 10 章 从病毒基本知识、病毒分析、病毒类型、新型病毒分析、各种操作系统病毒等方面介绍计算机病毒相关知识。

第 11 章 用户在使用网络资源时，需要了解针对各种计算机病毒和木马的防范方法。本章介绍了这些方法。

第 12 章 脚本攻击通常针对这些数据库来配合脚本对一些变量的过滤不严等问题，得到用户密码等敏感信息。本章就教会我们如何摆脱脚本攻击。

第 13 章 介绍防火墙的基本功能、工作原理、分类、体系结构、规则，随后介绍如何选择合适的防火墙和部分防火墙产品，在此基础上详细介绍了在不同操作系统平台下的防火墙软件的使用方法。

第 14 章 首先概述 IDS 的功能与模型、基本原理等，随后介绍产品选型原则及部分产品，然后着重介绍开源入侵检测系统 Snort，最后还阐述了入侵防御系统与 UTM 等未来发展方向。

第 15 章 让用户学习通过对网络的封锁和代理突破，来实现维护计算机网络的安全性和可靠性。

第 16 章 讲解针对计算机操作系统的攻防技术，以及如何实现对软件和文件资料进行加密等相关的内容。

第 17 章 讲解 ASP 和 PHP 环境下的 SQL 注入技术，并了解 SQL 注入的防护。

第 18 章 讲解在计算机网络安全的攻防中，使用欺骗攻击技术实施攻击的原理及其安全防范方面的相关知识。

第 19 章 讲解与后门技术相关的一些内容，使得读者对后门技术的攻击及防范知识有一定的了解。

第 20 章 介绍计算机取证的相关知识。计算机取证将计算机系统视为犯罪现场，运用先进的技术工具，按照规程全面检查计算机系统，提取、保护并分析与计算机犯罪相关的证据，以期据此提起诉讼。这一章从证据的获取和证据的分析两个方面结合相应软件进行了介绍。

第 21 章 介绍无线网络安全的内容，其中对无线访问设备、AP、无线网络协议、WEP 安全协议、NetStumbler 检测无线网络、无线网络的攻击及防护无线网络等知识进行了浅显的阐述。

本书读者

本书具有知识全面、实例精彩、指导性强的特点，力求以全面的知识性和丰富的实例来指导读者透彻学习计算机网络安全技术。本书适合作为对计算机网络安全感兴趣的读者的启蒙图书，也可以帮助具有一定技术程度的中级读者提高技能，对高级读者也有一定的启发意义。

本书作者

本书主要由李俊民、郭丽艳编写。其他参与编写的人员有张金霞、于锋、张伟、曾广平、刘海峰、刘涛、赵宝永、郑莲华、张涛、杨强、陈涛、罗渊文、李居英、郭永胜。在此对所有参与编写的人表示感谢！

由于笔者水平所限，书中可能还存在疏漏和错误，还望广大读者批评指正。

step 12 在显示的图片上单击鼠标右键，选择“属性”命令，打开如图 4.126 所示的对话框。

step 13 选中已经上传的木马在远程服务器中的地址并复制，如图 4.127 所示。

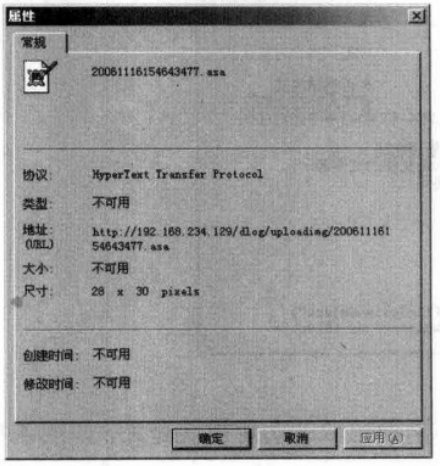

图 4.126 查看图片属性

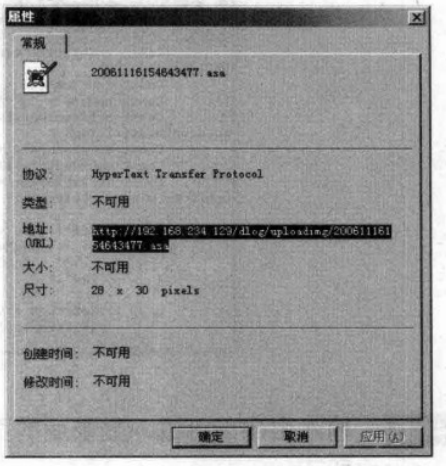

图 4.127 已经上传的木马的具体位置

step 14 新打开一个 IE 浏览器，在地址栏中粘贴找到的木马地址，如图 4.128 所示。

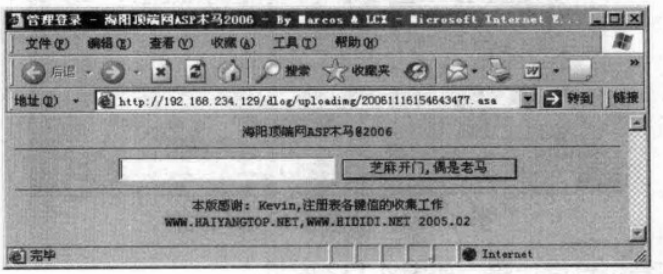

图 4.128 上传的 ASP 木马

step 15 在页面中的文本框中输入管理密码，默认密码为 lcxMarcos。此密码可以通过修改 2006.asp 文件取得，如图 4.129 所示。

图 4.129 2006.asp 文件

step 16 将 userpassword 行替换为自己指定的字符串，即可修改密码，如图 4.130 所示。

```
Const userpassword = "lcxMarcos"
```

图 4.130 替换字符串

step 17 输入密码即可进入登录后的页面。该页面的功能与前面选取的功能模块有关，如图 4.131 所示。

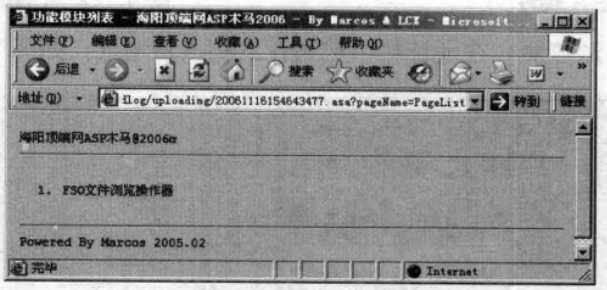

图 4.131 登录 ASP 木马文件

step 18 进入 FSO 文件浏览操作器，如图 4.132 所示。

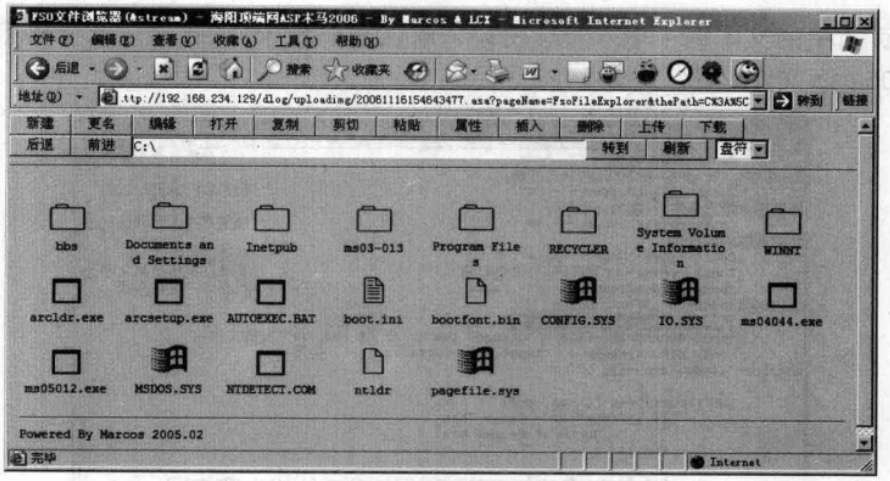

图 4.132 FSO 文件浏览操作器

4.3.5 安全解决方案

Dlog 的数据库漏洞在最新版本中已经完成了修补，可以从以下网址下载最新版本的安装程序。

```
http://www.duoluo.com/webdream/dlog/
```

也可以从以上网址下载旧版本的升级补丁程序。

4.4 基于 Cookie 欺骗的 Blog 入侵实例

Cookie 欺骗也是一种威胁比较严重的漏洞，主要原因是由于系统对 Cookie 信息验证不完全造成的。很多网站的主页都存在这样的漏洞。

4.4.1 漏洞的检测

本例中的攻击对象选择 L-Blog 系统，该系统操作简单，由于其使用开放源代码的方式，所以有很多版本，这里使用其中的一个版本。

为了找到该系统，可以使用搜索引擎 Google。

L-Blog 系统的一个可用关键字是“Powered By L-Blog”。利用这个关键字可以找到可能成为目标的 L-Blog 系统。但并不说明所有这些 L-Blog 系统都具有漏洞，可以尝试对这些论坛进行搜索以期发现可疑目标。

step 1 打开 IE 浏览器，在地址栏中输入 www.google.cn，按回车键打开 Google 主页，如图 4.133 所示。

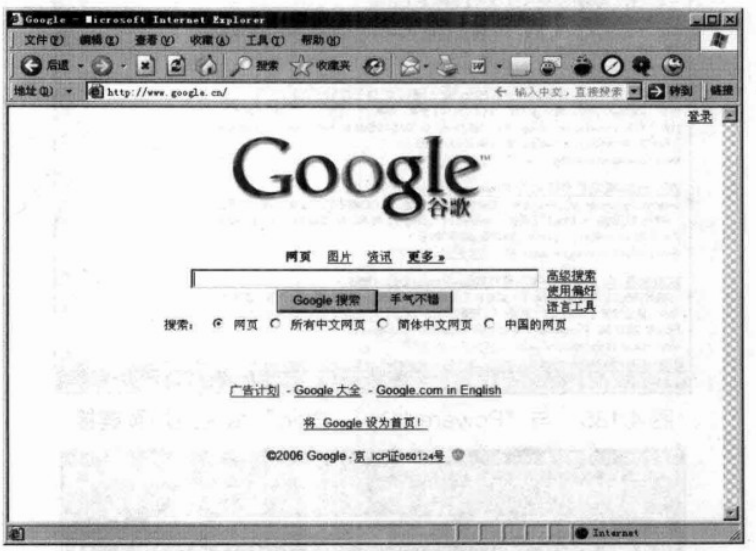

图 4.133 Google 主页

step 2 在搜索关键字文本框中输入如下关键字，注意该关键字包括了引号，如图 4.134 所示。

```
"Powered By L-Blog"
```

step 3 Google 会快速搜索所有与关键字“Powered By L-Blog”相关的网页链接，如图 4.135 所示。

step 4 一般来说，L-Blog 系统的版本都可能存在漏洞，所以可以从 Google 搜索的网页链接中找一个感兴趣的进行尝试，如图 4.136 所示。

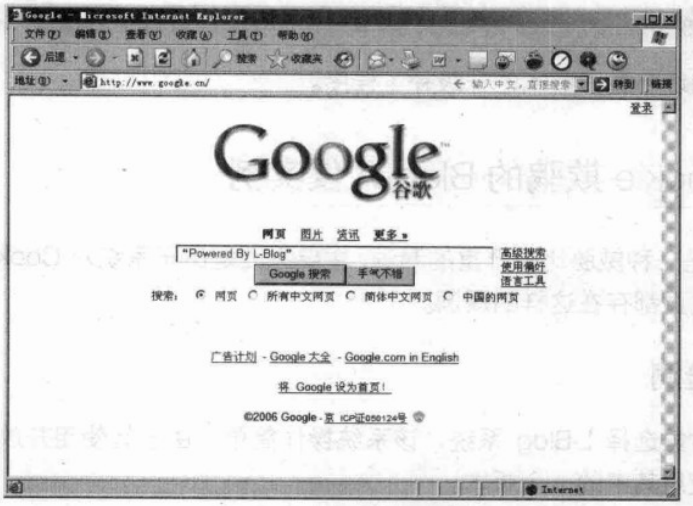

图 4.134 输入搜索关键字

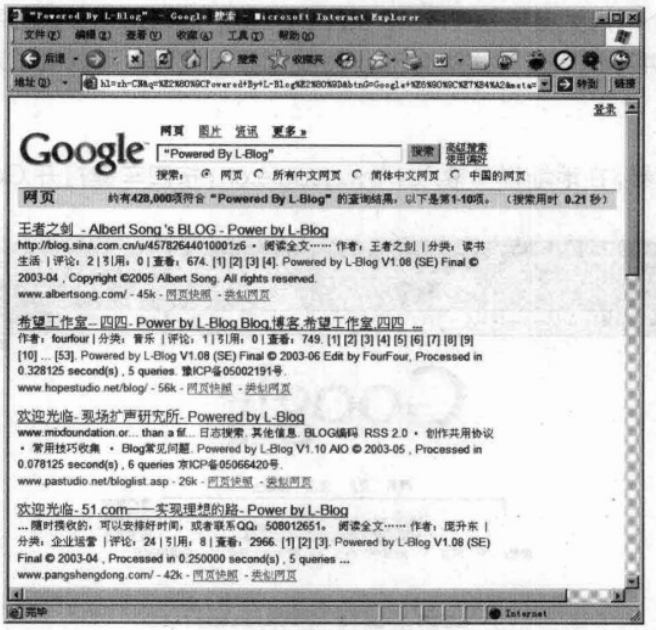

图 4.135 与“Powered By L-Blog”相关的网页链接

图 4.136 希望尝试的 L-Blog 系统

4.4.2 了解 L-Blog 系统的结构

下载一个 L-Blog 系统，该系统在下载完成以后并不需要安装，也是一个地道的绿色软件。使用解压缩软件，解压缩系统后的目录如图 4.137 所示。

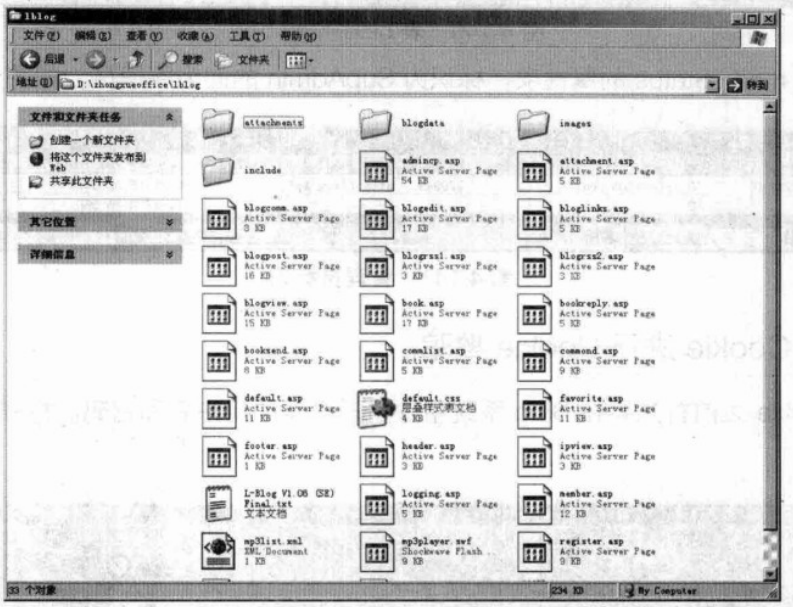

图 4.137 解压缩后的 L-Blog 系统

从 L-Blog 系统目录中找到一个名为 blogdata 文件夹，打开该文件夹，如图 4.138 所示。

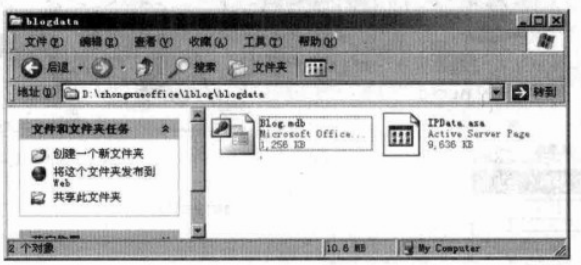

图 4.138 blogdata 文件夹

在该文件夹中找到一个名为 Blog.mdb 的数据库文件，使用微软 Access 数据库软件打开该文件，如图 4.139 所示。

图 4.139 Blog.mdb 数据库文件

在数据库文件中打开表 blog_Member，如图 4.140 所示。

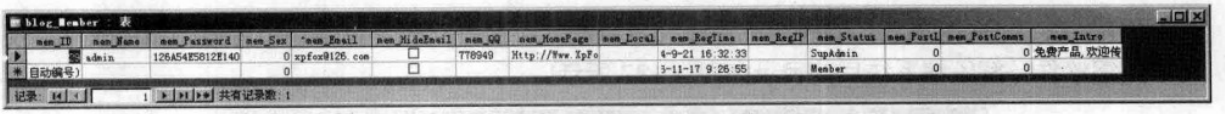

图 4.140 表 blog_Member

有一个名为 mem_Status 的属性项，标识为 SupAdmin 的即为管理员，如图 4.141 所示。

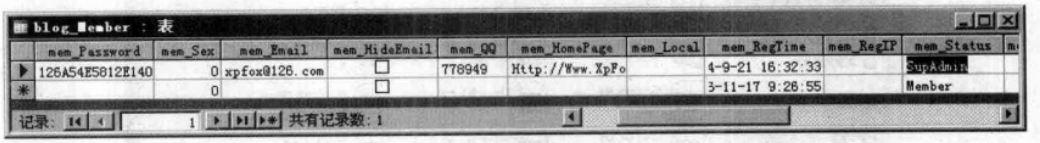

图 4.141 管理员标识

4.4.3 获取 Cookie 进行 Cookie 欺骗

在获取 Cookie 之前首先要在 Blog 系统中注册一个新的用户名和密码。打开 L-Blog 主页，如图 4.142 所示。

图 4.142 L-Blog 主页

通过注册，在 L-Blog 上拥有一个合法的权限。在此假设要注册的用户名是 upload，密码是 upload。

单击论坛首页的“注册”链接，打开注册声明页面，单击“我已阅读并同意以上条款”按钮，继续下一步，如图 4.143 所示。

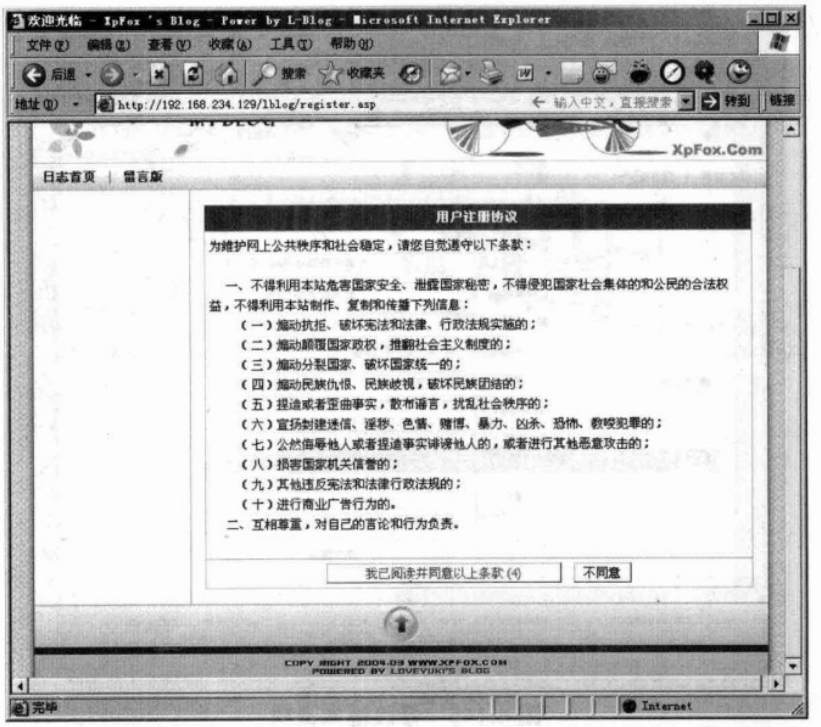

图 4.143　同意注册协议

在注册用户信息页面中输入刚才确定的用户名和密码并完成其余内容的输入，提交论坛系统审核，如图 4.144 所示。

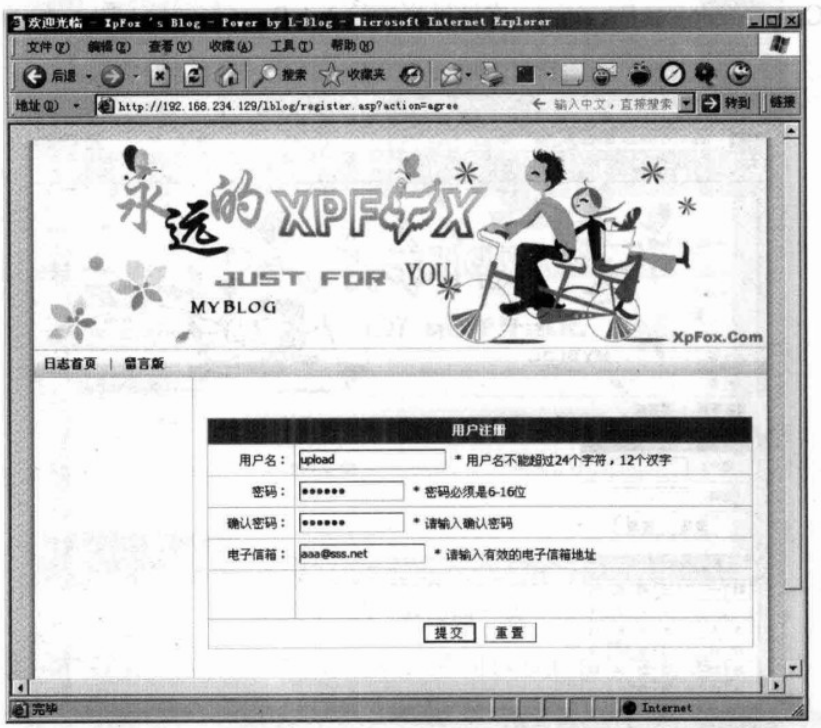

图 4.144　注册用户信息

在确认注册完成之后，也可以登录用户控制面板中的基本资料修改页面进行修改，如图 4.145 所示。

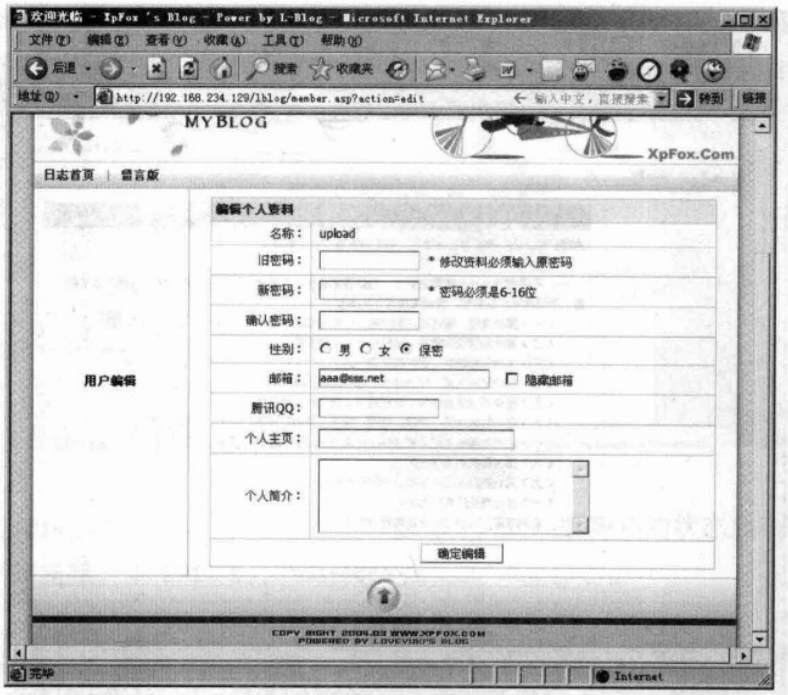

图 4.145 修改基本资料

接下来需要使用新的 Cookie 工具，这里选用桂林老兵的 Cookies&Inject Browser，该工具与以前使用的工具类似。

step 1 打开 Cookies&Inject Browser，在地址栏中输入 L-Blog 系统的 URL，如图 4.146 所示。

图 4.146 使用 Cookies&Inject Browser 打开 L-Blog 系统

step 2 在登录文本框中输入刚才注册的用户名和密码，登录成功，如图 4.147 所示。

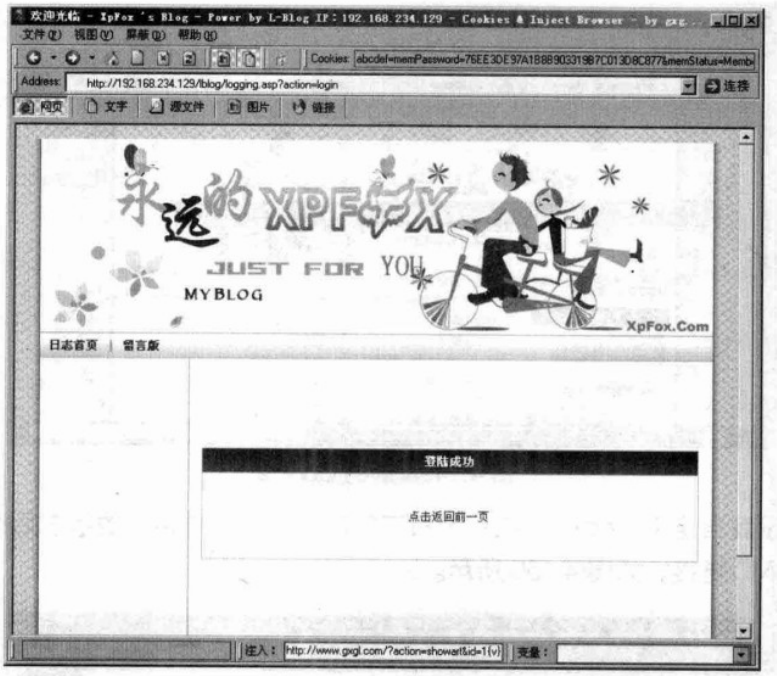

图 4.147 登录成功

step 3 单击“点击返回前一页”链接，显示的页面如图 4.148 所示。

图 4.148 返回前一页

step 4 注意在工具栏右侧显示了 Cookie 信息，从中可以找到如下字符串：

```
memStatus=Member
```

Member 表示普通用户。前面得到了该系统的管理员标识 SupAdmin，可以将 Member 改为 SupAdmin，Cookie 也随之改变，如图 4.149 所示。