高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材

Web安全程序设计与实践

主编　孙海峰
参编　黄晓芳　覃仁超　黄　洪

西安电子科技大学出版社
http://www.xduph.com

高等学校电子信息类“十三五”规划教材

应用型网络与信息安全工程技术人才培养系列教材

Web 安全程序设计与实践

主　编　孙海峰

参　编　黄晓芳　覃仁超　黄　洪

西安电子科技大学出版社

内 容 简 介

本书主要讲述 Web 安全漏洞的分析与防护。全书共分为四篇，第一篇为预备知识，包括 Web 服务器平台安装与配置和 Web 开发基础两个项目；第二篇为 SQL 注入攻击及防护，包括万能密码登录——Post 型注入攻击、数据库暴库——Get 型注入攻击、更新密码——二阶注入攻击、Cookie 注入攻击和 HTTP 头部注入攻击五个项目；第三篇为前端攻击及防护，包括 Session 欺骗攻击、Cookie 欺骗攻击、XSS 跨站攻击、CSRF 跨站伪造请求攻击和验证码五个项目；第四篇为文件漏洞及防护，包括文件上传漏洞、文件下载漏洞、文件解析漏洞和文件包含漏洞四个项目。

本书可作为普通高校计算机及相关专业学生学习 Web 程序设计的教材或参考书，也可供从事 Web 程序设计的技术人员学习和参考。

图书在版编目(CIP)数据

Web 安全程序设计与实践 / 孙海峰主编. —西安：西安电子科技大学出版社，2019.4
ISBN 978-7-5606-5297-9

Ⅰ. ① W… Ⅱ. ① 孙… Ⅲ. ① 互联网络—安全技术 ② 网页制作工具—程序设计
Ⅳ. ① TP393.408 ② TP393.092.2

中国版本图书馆 CIP 数据核字(2018)第 051252 号

策划编辑 李惠萍
责任编辑 唐小玉
出版发行 西安电子科技大学出版社(西安市太白南路 2 号)
电 话 (029)88242885 88201467 邮 编 710071
网 址 www.xduph.com 电子邮箱 xdupfxb001@163.com
经 销 新华书店
印刷单位 咸阳华盛印务有限责任公司
版 次 2019 年 4 月第 1 版 2019 年 4 月第 1 次印刷
开 本 787 毫米×1092 毫米 1/16 印 张 13.5
字 数 316 千字
印 数 1～3000 册
定 价 34.00 元

ISBN 978-7-5606-5297-9 / TP

XDUP 5599001-1

前　言

1991 年，图灵奖获得者、万维网之父、万维网联盟的创建者蒂姆·伯纳斯-李(Tim Berners-Lee)正式公开发布了全世界第一个网页。根据 Netcraft 的统计，到 2017 年底，全球活动网站数量已经超过一亿个。根据中国互联网协会统计，中国的网站数量已经超过 500 万个。从其迅猛发展的过程可知网站在信息时代的地位和它对社会发展起到的重要作用。

随着网站的广泛普及与应用，网站安全入侵事件也变得层出不穷，商业网站、政府网站、大学和教育部门的网站被黑客攻击造成的损失更是难以统计。从国家信息安全漏洞报告平台、乌云网(WooYun，自 2016 年 7 月 20 日停止服务)等一些互联网漏洞报告平台公开的信息可知，出现安全漏洞的网站数量之广泛、问题之严重已达到惊人的地步。在赛门铁克 2015 年扫描的网站中，有四分之三的网站存在漏洞。全球最大的社交网站 Facebook 在 2018 年 9 月 28 日表示遭到黑客攻击，涉及近 5000 万用户；即使 FBI、五角大楼的网站也不能幸免。2013 年，美国、荷兰等十余个国家的银行系统遭受攻击，黑客“黑”进银行预付借记卡系统，盗取了 4500 万美元。2015 年 5 月 28 日，国内某大型在线票务服务公司官网出现大面积瘫痪，瘫痪每小时损失高达 106.5 万美元。受此影响，其股价盘前暴跌 11.67%。2017 年，我国公安系统破获了一起黑客攻击窃取国内航空公司网站信息的特大型案件。在该起案件中，黑客非法入侵 50 多家民用航空类公司网站，窃取乘客票务信息，再利用这些信息实施网络诈骗，骗取受害者资金累计金额高达 1000 多万元。

网站之所以遭到攻击，主要是因为存在一些安全漏洞，如 SQL 注入漏洞、跨站脚本攻击漏洞等。本书希望通过作者精心设计的项目案例起到抛砖引玉的作用，使网站开发程序员认识到网站漏洞的危害，掌握常见的网站攻击原理和防御手段，建立网站安全意识，重视安全测试和代码审计工作。特别需要注意的是网站的安全是一个系统工程，它还涉及主机安全、操作系统安全、网络安全、容灾备份等方面，代码安全只是满足系统安全的一个方面。

本书以项目为依托，通过重现网站漏洞，并在此基础上进行漏洞测试与防护，以满足实际的 Web 安全技术学习的需求和国家法律要求。据权威统计，在所有运行的网站中，PHP 语言设计的网站占有的比例超过了 80%，而 Apache 在 Web 服务器市场占有率排名第一。因此，本书从网站开发的角度，以 Apache 和 PHP 组合作为 Web 服务器来具体阐述 Web 安全防护问题。但是，不管网站的开发语言使用的是 PHP、JSP、ASP、Python 语言还是 reviewer EE 架构，不管是前后端混合还是前后端分离，不管是使用 MVC 模型还是 RESTful 风格，都面临着同样的安全威胁。所以，本书对其他 Web 编程语言和 Web 服务器平台的安全防护，仍然有重要的参考价值。

需要特别提醒的是，除非在获得合法授权的情况下，网站安全漏洞测试不能在商业网站或者政府、教育机构等单位的网站进行。《中华人民共和国刑法》第二百八十五条规定了非法侵入计算机信息系统罪，第二百八十六条规定了破坏计算机信息系统罪。《中华人民共和国治安管理处罚法》第二十九条规定了违反国家规定，侵入计算机信息系统等行为的处

罚标准。此外，《中华人民共和国网络安全法》、《中华人民共和国电信条例》等法律法规均禁止破坏信息系统的行为。另一方面，国家法律也规定了网络运营者有维护网络安全的义务和责任，经监管部门责令采取改正措施而拒不改正者将受到法律的制裁。

本书共包括四篇十六个项目，第一篇为预备知识，包括 Web 服务器平台安装与配置和 Web 开发基础两个项目；第二篇为 SQL 注入攻击及防护，包括万能密码登录——Post 型注入攻击、数据库暴库——Get 型注入攻击、更新密码——二阶注入攻击、Cookie 注入攻击和 HTTP 头部注入攻击五个项目；第三篇为前端攻击及防护，包括 Session 欺骗攻击、Cookie 欺骗攻击、XSS 跨站攻击、CSRF 跨站伪造请求攻击和验证码五个项目；第四篇为文件漏洞及防护，包括文件上传漏洞、文件下载漏洞、文件解析漏洞和文件包含漏洞四个项目。

本书在编写期间得到了编者所在单位师生的大力配合和协助，在此表示衷心的感谢！同时也要感谢出版社编辑们的耐心交流与指导，使得本书能够顺利与读者见面。

由于作者水平有限以及编写时间仓促，书中难免会出现一些疏漏或不足之处，恳请读者批评指正，使我们共同进步。欢迎您通过西安电子科技大学出版社网站与笔者联系，也欢迎直接与笔者交流，笔者的邮箱是 dr_hfsun@163.com。

作　者

2019 年 1 月

目　录

第一篇　预 备 知 识

第二篇　SQL 注入攻击及防护

第三篇 前端攻击及防护

第四篇　文件漏洞及防护

第一篇 预备知识

Web 服务器平台的组合多种多样，主要包含操作系统、Web 服务器软件和数据库三大部分。本书从市场占有率、易操作性和使用成本三个方面综合考虑，采用了 Windows Server 2008 操作系统、Apache(Apache HTTP Server，简称 Apache Web 服务器)、PHP 和 MySQL 数据库的组合。其中 Apache 只能解析静态的 HTML 网页；PHP 是负责解析 PHP 语言编写的网页文件的解释器，要和 Apache 以 CGI 等方式结合起来才能处理访问请求。

本篇包含两个项目，首先是 Web 服务器平台的安装与配置，这为本书项目的实施搭建了基础平台。主要内容包括 Windows Server 2008 企业版操作系统、PHP、MySQL 数据库和 Apache Web 服务器的安装与配置。本书在软件或者插件选型上尽量选用高版本系统，这样一方面可以满足长期使用的需求，另一方面也可使面临的 Web 安全问题更加具有普遍意义。接下来是 Web 开发基础，主要包括 SQL 语言基础和 MySQL 数据库的操作基础，HTML 与 CSS 标记语言、JavaScript 脚本语言以及 PHP 脚本语言的基本知识和基本应用。

通过本篇两个项目的实训，实现配置和使用 Web 服务器平台、进行基本的 PHP 动态网页开发等目标。

项目 1 Web 服务器平台安装与配置

【项目描述】

本项目对 Web 服务器平台的安装和配置进行实训，项目包含四个任务，首先安装 Windows Server 2008 企业版操作系统，然后依次对 PHP 软件包、MySQL 数据库和 Apache Web 服务器进行安装与配置。

通过本项目的实训，读者可以熟悉 Web 服务器平台的主流组合方式以及 Web 服务器平台的构成，掌握 Web 服务器平台的安装与配置。

【知识储备】

Web 服务器平台的组合多种多样。本书搭建的 Web 服务器环境操作系统选用 Windows Server 2008 简体中文企业版，Web 服务器使用 Apache 2.4 和 PHP 7.1，数据库使用 MySQL 5.5。下面分别对这些 Web 服务器的平台组件进行简要说明。

1. Windows Server

常见的服务器操作系统有 Microsoft Windows Server、Linux/Unix 等。根据 W3Techs[①]的统计，截至 2018 年 3 月 26 日，在网站所采用的操作系统中，32.8%为 Windows 操作系统，而 67.2%为 Unix/Linux/BSD 等操作系统。Unix/Linux 操作系统和这些系统下运行的软件几乎都是免费使用的，而且性能优异，但是用户需要有一定的基础才能熟练掌握并使用它们。

Windows Server 系列的操作系统是微软推出的商业服务器操作系统。对于普通用户来说，Windows 操作系统可以在纯图形界面下操作使用，依靠鼠标和键盘完成一切操作，上手容易，入门简单。本书选用的 Web 服务器操作系统为 32 位的 Windows Server 2008 简体中文企业版。

2. Apache

常见的 Web 服务器有 Apache、Microsoft IIS、Nginx 等。其中，Apache 是 Apache 软件基金会(Apache Software Foundation，ASF)的 HTTP Server 项目，取名于北美的一个印第安人部落名称。Microsoft IIS 属于微软公司的 HTTP Server 商业软件产品，对比开源软件，商业软件提供的售后服务是其优势。Nginx 采用的开源项目许可证是 2-clause BSD-like license，其特点是占有内存少，并发能力强。

Apache 软件基金会的项目都遵循 Apache 许可证[②]。由于其开源特点，得到了开源社区

---

① 提供关于互联网不同技术运用信息的调查网站 https://w3techs.com/。

② Apache 许可证属于开源许可证之一，其他比较出名的还有 GPL、BSD、MIT、MPL 和 LGPL 等。

的大力支持，吸引了众多优秀的开发人员参与其中，他们不断开发出各种新的功能，并对存在的缺陷进行修复，以提高其效率和稳定性。经过多年的不断完善，如今的 Apache 已经是最流行的 Web 服务器端软件之一。截至 2018 年 3 月 26 日，根据 W3Techs 对 Web 服务器市场份额的统计，排名第一的 Apache 占据了 47.0%的比例，排名第二和第三的 Nginx 和 Microsoft IIS 分别占据了 37.7%和 10.0%。根据 Netcraft 对 Web 服务器市场份额从 2000 年 6 月一直到 2017 年 12 月的统计数据[1]，Apache 服务器始终稳居活动网站的第一名，如图 1-1 所示。本书使用的 Web 服务器为 Apache 2.4.33。

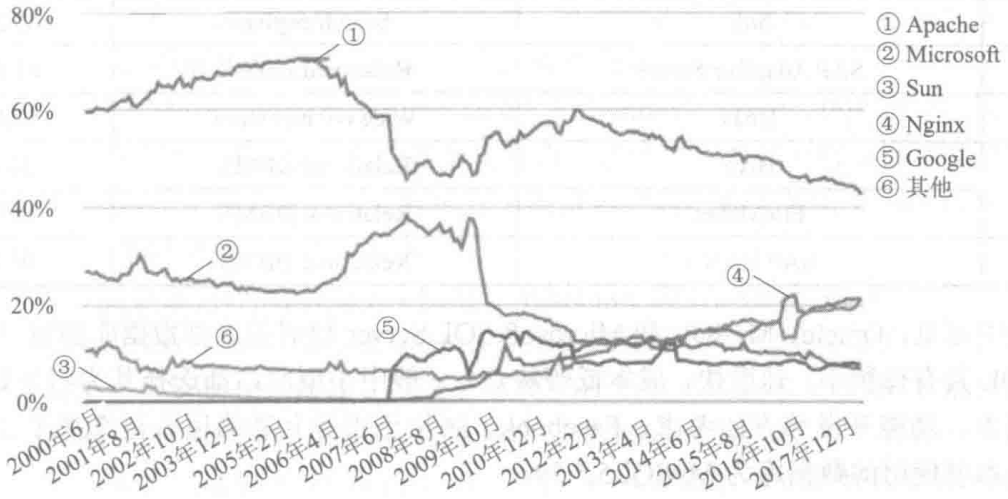

图 1-1 W3Techs 统计的 Web 服务器市场份额

3. MySQL 数据库

当前主流的关系型数据库管理系统(Relational Database Management System，RDBMS)中，商业数据库有 Oracle、Microsoft SQL Server、IBM DB2 等，开源数据库包括 MySQL 社区版、PostgreSQL 等。MongoDB、Redis、Memchache 则是常用的非关系型数据库(NoSQL)。DB-Engines[①]使用搜索结果的数量、总体兴趣、技术讨论频率等标准，对 300 多种数据库管理系统产品进行统计排名，其中前 20 名的排名结果如表 1-1 所示。

表 1-1 DB-Engines 统计的数据库管理系统产品排名(2018 年 4 月数据)

排名	数据库管理系统	数据库模型	得分
1	Oracle	Relational DBMS	1289.79
2	MySQL	Relational DBMS	1226.4
3	Microsoft SQL Server	Relational DBMS	1095.51
4	PostgreSQL	Relational DBMS	395.47
5	MongoDB	Document store	341.41
6	DB2	Relational DBMS	188.95
7	Microsoft Access	Relational DBMS	132.22
8	Elasticsearch	Search engine	131.36
9	Redis	Key-value store	130.11

① https://db-engines.com/en/ranking

续表

排名	数据库管理系统	数据库模型	得分
10	Cassandra	Wide column store	119.09
11	SQLite	Relational DBMS	115.99
12	Teradata	Relational DBMS	73.68
13	Splunk	Search engine	65.06
14	MariaDB	Relational DBMS	64.56
15	Solr	Search engine	63.21
16	SAP Adaptive Server	Relational DBMS	61.63
17	Hbas	Wide column store	59.69
18	Hive	Relational DBMS	57.4
19	FileMaker	Relational DBMS	55
20	SAP HANA	Relational DBMS	48.9

从表中可见，Oracle、MySQL 和 Microsoft SQL Server 稳居关系型数据库的前三名。由于 MySQL 具有体积小，速度快，成本低等特点，一般中小型网站都选择其为网站数据库。从使用成本、功能开发等方面考虑，Facebook、阿里巴巴等互联网巨头也选择了 MySQL 数据库。本书使用的数据库为 MySQL5.5.59。

4. PHP 语言和 PHP 解释器

常见的服务器端编程语言有 PHP、ASP、ASP.NET、Java 等。截至 2018 年 3 月 26 日，根据 W3Techs 对于服务器端编程语言的统计，83.2%的网站使用 PHP 语言，ASP.NET 和 Java 则分别占有 13.8%和 2.3%。

PHP 原为 Personal Home Page 的缩写，后更名为“PHP: Hypertext Preprocessor”，是一种通用开源脚本语言。PHP 的语法吸收了 C 语言、Java 和 Perl 的特点，入门简单，开发效率高，主要适用于 Web 开发领域。

PHP 解释器负责解释 PHP 语言编写的脚本文件，本书使用的 PHP 解释器版本为 PHP 7.1.16。

PHP 程序的集成开发环境开发工具有免费的 Eclipse with PDT，也有商业版的 PHP Storm 等。本书的重点不在 PHP 程序开发，故使用 NodePad++来编写 PHP 和 HTML 等文件。

任务 1-1　安装 Web 服务器操作系统

本任务是进行 Windows Server 2008 简体中文企业版操作系统的安装。

一方面，由于目前实验室中仍存在大量的 32 位操作系统的计算机，而在 Windows Server 2008 服务器操作系统诞生之后，微软公司就不再开发 32 位的 X86 服务器操作系统了，因此本书使用 32 位 Windows Server 2008 简体中文企业版操作系统的 SP2 版本。另一方面，本书使用的软件如 Apache、MySQL 等，在 64 位 Web 服务器操作系统中的配置使用与 32 位系统大同小异，甚至也可以在 Windows 10 操作系统中进行开发和测试。对于有一定

Linux/Unix 操作系统使用经验的读者，推荐使用 CentOS、Ununtu 等作为 Web 服务器操作系统。

推荐采用 VMware 软件的方式安装 Windows Server 2008 操作系统。在 VMware 中运行的操作系统称之为虚拟机，安装并运行了 VMware 虚拟机的操作系统称为宿主机。由于 VMware Workstation Pro 10 是支持 32 位操作系统的最后一个版本，因此本书使用 VMware Workstation Pro 10.0.7 版本的个人桌面版虚拟机软件。如果使用 64 位操作系统的计算机，推荐选用 VMware Workstation Pro 14 安装 Windows Server 2016 企业版操作系统的虚拟机，请在参考本书提供的安装步骤基础上自行实现。在实际的生产环境中，从系统安全角度等方面考虑，建议选用最新版的 Windows Server 操作系统。

请自行安装 VMware Workstation Pro 10.0.7 和 Windows Server 2008 企业版操作系统虚拟机作为 Web 服务器，并将虚拟机的网卡设置为桥接模式。本书中的项目可以在虚拟机中进行测试；如果将宿主机或者其他计算机作为测试客户端，推荐关闭 Windows Server 2008 虚拟机操作系统的防火墙，以免访问被拦截。

由于 Web 服务器软件 Apache 2.4 使用了 Windows 10 Universal CRT 的功能[①]，而微软提供了 Windows Server 2008 SP2 版本的 Universal CRT 补丁，如果安装的 Windows Server 2008 企业版操作系统是 SP1 版本，需要首先将操作系统升级到 SP2 版本(如果直接安装了 Windows Server 2008 SP2 操作系统，则可以忽略此步骤)。升级到 SP2 版本后再安装 Universal CRT 补丁 Windows 6.0-KB2999226-x86.msu 即可。Web 服务器操作系统信息如图 1-2 所示。

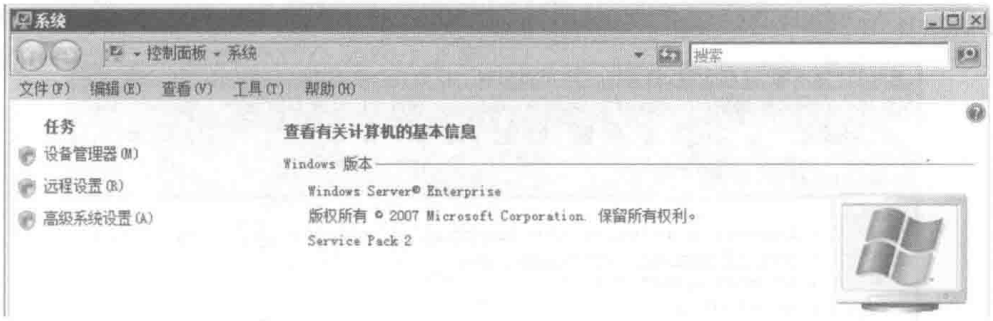

图 1-2 操作系统信息

实施本书的项目和任务需要安装使用三种浏览器：自带的 IE 浏览器(7.0 版本)、Firefox 浏览器(52.8.0 版本)和 360 安全浏览器(9.1.0.434 版本)。另外，还需要安装 Notepad++(7.5.6 版本)，用以编辑网页。

扩展阅读

网站的开发环境、生产环境和测试环境

网站的开发环境是指用于网站开发的服务器。为了开发调试方便，需要打开网站的全部错误报告功能。生产环境是网站运行的正式环境，正式对外提供服务，被用户所使用，

① https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows。

因此注重网站运行的性能和安全性。在生产环境中会关掉错误报告，通过错误日志文件的方式监控网站运行。测试环境与生产环境的配置一致，是开发环境到生产环境的过渡环境，用于进行网站的功能和性能等的测试，主要用于测试网站的功能是否符合需求，是否存在错误和漏洞，性能是否达到指标等。

任务 1-2　安装并配置 PHP

本任务下载安装并配置 PHP 及依赖的运行环境，所使用的版本为 7.1.16。

在 PHP 官网下载 VC14 x86 Thread Safe 版本 php-7.1.16-Win32-VC14-x86.zip，将其解压到 C:\php-7.1.16-Win32-VC14-x86。其中 VC14 表示是使用 Visual Studio 2015 编译的版本，因此需要首先安装 Microsoft Visual C++ 2015 运行环境 Visual C++ Redistributable for Visual Studio 2015_x86.exe，配置步骤如下：

1. 生成配置文件 php.ini

进入目录 C:\php-7.1.16-Win32-VC14-x86，复制一份 php.ini-development 文件，并将其重命名为 php.ini。

2. 更改配置文件的自定义扩展目录

打开 php.ini 找到;extension_dir = "ext"，去掉前面的分号(分号表示注释，该行不起作用)，并更改为 extension_dir = "C:\php-7.1.16-Win32-VC14-x86\ext"，如图 1-3 所示。

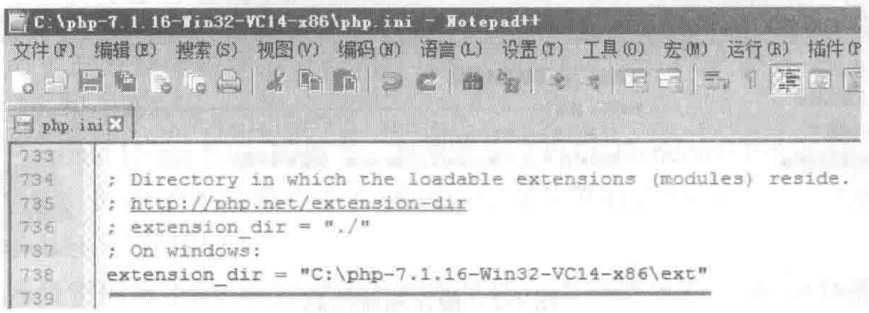

图 1-3　更改 PHP 自定义扩展目录

3. 开启 php_mysqli 扩展的动态链接库

在 php.ini 中找到如下内容并去掉分号注释：

```
;extension=php_mysqli.dll
```

php_mysqli 是 PHP5 之后的版本推荐使用的数据库扩展。

4. 设置错误报警级别

在 php.ini 中找到 display_errors = Off，将其修改为 display_errors = On。

找到 error_reporting = E_ALL，在后面增加 ^ E_DEPRECATED，即

```
error_reporting = E_ALL ^ E_DEPRECATED
```

其作用是报告 PHP 脚本除了过时函数之外的其他所有错误。

重点：这种错误报警配置属于开发环境的设置。如果是在生产环境，一定要关闭错误报警，以防别人利用错误来实施攻击。

注意：每次修改 php.ini 文件后都需要重新启动 Apache 服务。Apache 服务的安装和配置过程会在后续的小节给出。

任务 1-3 安装并配置 MySQL

本任务下载安装并配置 MySQL 数据库软件。

从官网下载 MySQL，可以选择 msi 安装版，也可以选择 zip 免安装版。本书使用的版本为免安装 5.5.59-win32 版本，安装配置过程如下：

1. 解压软件包

将 mysql-5.5.59-win32.zip 压缩包解压到 C:\mysql-5.5.59-win32。

2. 生成配置文件 my.ini

在 C:\mysql-5.5.59-win32\bin 复制配置文件 my-small.ini，重新命名为 my.ini，在[client]部分添加默认字符集为 default-character-set=utf8，在[mysqld]部分添加 MySQL 的安装目录等内容，具体如下：

```
basedir=C:\mysql-5.5.59-win32
#设置 mysql 的数据目录
datadir=C:\mysql-5.5.59-win32\data
character_set_server=utf8
```

MySQL 配置文件的修改部分如图 1-4 所示。

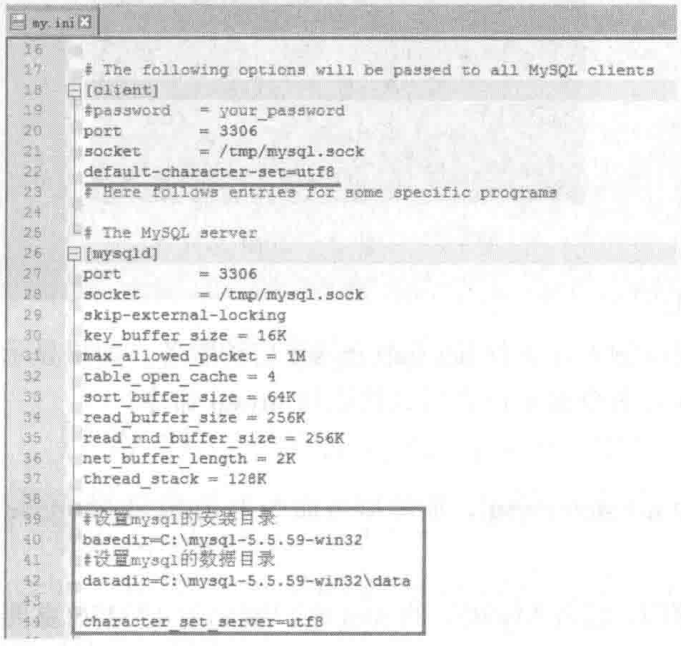

图 1-4 MySQL 配置文件设置

3. 给 MySQL 配置环境变量

右键打开桌面“我的电脑”对话框，点击“高级系统设置”按钮，在“高级”选项卡中点击“环境变量”按钮；在“系统变量”中选中“path”，点击“编辑”按钮，在“变量

值”文本框的最后添加；C:\mysql-5.5.59-win32\bin，并依次点击“确定”按钮，完成 MySQL 的环境变量设置，如图 1-5 所示。

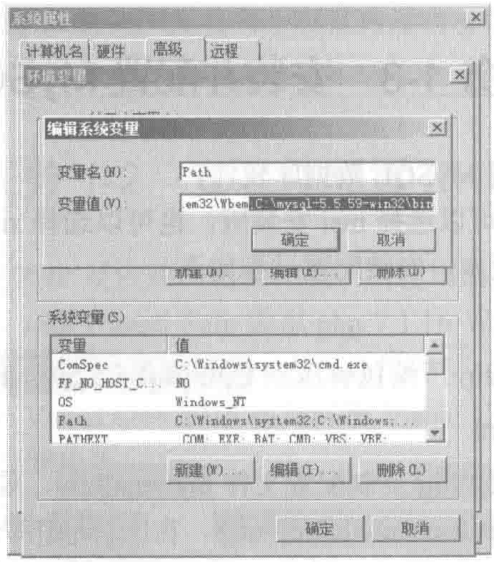

图 1-5　设置 MySQL 环境变量

4. 将 MySQL 注册为系统服务

在命令提示符窗口，进入 C:\mysql-5.5.59-win32\bin 目录，输入并运行 mysqld --install mysql。如果提示“Service successfully installed”，则表示服务安装成功，如图 1-6 所示。

图 1-6　安装并启动 MySQL

5. 启动 MySQL

在命令提示符窗口输入并运行 net start mysql 启动服务。如果显示 MySQL 服务已经启动成功，就可以在打开命令提示符之后直接运行 mysql 命令。

6. 其他操作

停止服务命令为 net stop mysql，删除服务命令为 mysqld --remove。

7. 设置密码

在命令提示符窗口，修改 MySQL 的 root 账户密码为 123456(**重要**：在生产环境中该密码必须要设置成比较复杂的密码，以增加系统安全性)，命令为 mysqladmin -u root password 123456。

8. 登录 MySQL

在命令提示符窗口输入 mysql -uroot -p 和密码。如果出现图 1-7 所示界面信息，则表示