基于JSP商品销售系统的实现与安全设计

杨 军
(盐城工学院 招生就业处,江苏 盐城 224051)

摘要:描述了JSP的特点和优势以及利用它怎样来实现在商品销售系统。给出了系统的需求分析和功能实现。特别介绍了怎么样运用字符过滤技术和md5单向加密算法和随机算法以及JSP的Session对象来实现安全设计。

关键词:JSP;安全设计;商品销售系统
中图分类号:TP302.1 文献标识码:A 文章编号:1671-5322(2008)03-0034-03

1 JSP简介

1.1 JSP(Java Server Pages)简介

JSP是一种将静态HTML和动态的HTML巧妙集合起来的服务器端脚本技术[1-2]。访问JSP文件主要有两种方法:一种是浏览器发送对JSP文件的请求,JSP调用Bean组件执行任务,并将生成的内容发到浏览器组件;另外一种是客户端直接将请求发送至Servlet,由Servlet负责生成动态内容,再激活一个JSP文件来显示所生成的内容,两种访问JSP的方法见图1。

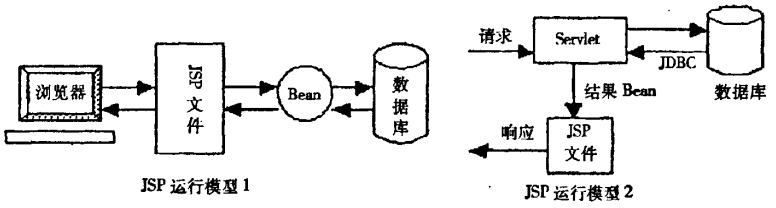

图1 访问JSP文件的方法

Fig. 1 The method of accessing JSP file

1.2 JSP的优点

(1)将内容的产生和显示进行分离

使用JSP技术,Web页面开发人员可以使用HTML或者XML标识来设计和格式化最终页面。使用JSP标识或者小脚本来产生页面上的动态内容。产生内容的逻辑被封装在标识和JavaBeans群组件中,并且捆绑在小脚本中,所有的脚本在服务器端执行。

(2)强调可重用的群组件

绝大多数JSP页面依赖于可重用而且跨平台的组件(如:JavaBeans或者Enterprise JavaBeans)来执行应用程序所要求的更为复杂的处理。

(3)采用标识简化页面开发

JSP技术封装了许多功能,这些功能是在易用的、与JSP相关的XML标识中进行动态内容产生所需要的。作为Java平台的一部分,JSP拥有Java程序设计语言"一次编写,各处执行"的特点。

2 系统的需求分析

2.1 系统的需求分析的功能

系统的需求分析是软件设计中极其重要的一个环节,按照系统的思想,根据收集的资料,对系统目标进行分析,对业务的信息需求、功能需求、

收稿日期:2008-03-19

作者简介:杨军(1969-),男,江苏建湖人,讲师,硕士,主要研究方向为计算机应用。

万方数据

辅助决策需求以及管理中可能存在的问题等进行分析,抽取现行系统本质的、整体的需求,为设计一个结构良好的新系统逻辑模型奠定了基础。

2.2 系统要实现的功能

系统实现了对商品的划价管理,销售管理,打印库存单,销售单,商品销售数据统计报表和打印统计(包含日结统计和月结统计),客户资料录入和公司部门及员工资料管理。系统可以同时进行商品进货、进货划价、库存 管理、系统维护,日常营业收费和统计查询等,商品收费的同时系统会自动的计算每个商品的纯利润和总纯利 润,同时随着仓库中商品[库存量]逐步地减少,系统会及时的提示、警告库存量不足等。

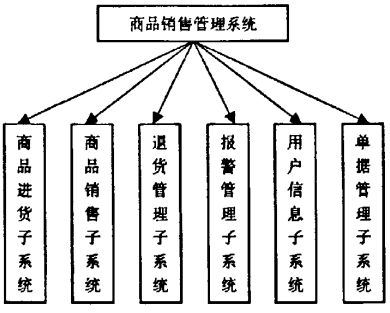

图2　系统模块图

Fig.2　System Module

2.3 系统的功能模块

本系统主要分为6个子系统,如图2所示。每个子系统基本都有如图3的功能模块。

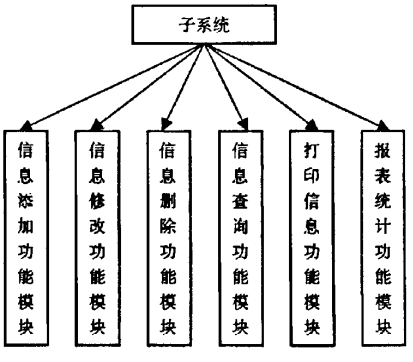

图3　子系统模块图

Fig.3　Subsystem Module

3 系统的设计与实现

3.1 系统的设计与实现的功能

系统的设计与实现是本系统的关键所在,在这里我们实现了各个子模块的核心功能。这里面涉及到大量的JSP代码和Java Bean代码(如连接数据库Java Bean,分页JavaBean),在此限于篇幅不便详细列出,我们只描述整个系统实现的思路。

3.2 信息上传

通过链接(links)跳转到信息上传页面,填写好各项需要填写的信息,点击确定按钮即可上传信息。这个模块我们用到了SQL语句,相信大家对此已经非常的熟悉,就不再列出,同时我们还运用了在线HTML编辑器eWebEditor JSP版,她能够在网页上实现许多桌面编辑软件(如:Word)所具有的强大可视编辑功能;她是一个真正的绿色软件,不需要在计算机上安装任何的客户端软件。她的易用使得Web开发人员只要一行代码即可完成调用[3]。

3.3 信息修改

通过链接(links)

<a href="modify.jsp?id=<%=rs.getInt("news_id")%>">修改得到需要修改的资料的id(主码),连接数据库,得到相应资料的全部信息,显示在网页控件中,然后做出修改,最后点击修改按钮将新的信息送往数据库,然后关闭数据库。实现信息修改。

3.4 信息删除

当点击删除链接(links)<a onClick="return confirm('真的要删除吗?')" href="del.jsp?id=<%=rs.getInt("news_id")%>">d删除时弹出是否删除对话框,如果选择是,通过参数传递得到需要修改的资料的id(主码),连接数据库,删除资料信息。否则返回资料显示页面。

3.5 信息搜索

信息查询功能实现了单条件查询和多条件查询,模糊查询融于条件查询中。可以对某一表的所有字段进行任意的组合查询,而且每个条件可以是模糊的,各条件间可以是"逻辑和"的关系,也可以是"逻辑与"的关系,最后形成查询条件,进行信息检索和工作统计。

在搜索条件栏中输入搜索关键字,通过表单进行数据传输,首先验证查询条件是否正确。如果正确则组合成查询条件,连接数据库,将查询语

万方数据

句送往数据库,服务器回应,得到我们想要的检索信息,否则返回搜索页面重新输入查询条件[4-5]。

4 安全性设计

4.1 防范SQL注入

本系统通过JDBC连接SQL SERVER 2000数据库。系统中通过使用用户资格认证,要求用户输入用户名和密码,达到加密内部网页的目的。然而,用户输入一些特殊的字符,使得认证系统失效。假设admin是数据表名,表中的字段有username(用户名)和password(密码)。在用户登录时,用户输入用户名和密码后,系统会执行这样一条SQL语句:

String sql = "select * from admin where user name = '" + uid + "' and password = '" + pwd + "'"

如果用户输入用户名为:' or 1 = 1 - -,密码为任意的字符,此时执行的SQL语句为:

String sql = "select * from admin where username = '' or 1 = 1 - - and password = ''",

'- -'符号在Transact - SQL中表示注释,那么'- -以后的语句就会被忽略,这样SQL语句相当于:

String sql = "select * from admin where username = '' or 1 = 1",

由于运算符or和"1 = 1"恒成立,因此得出数据库中有该用户的错误结果。当然上面只是SQL注入的一种。本系统对此问题进行了很好的解决,在用户登录输入用户名和密码后,系统运用JavaScript进行了字符过滤,如果用户输入的字符中有空格、"'"及"- -"中的一种,就判定为非法输入,要求用户重新输入。同时还运用JavaScript限制字符输入的个数,这样也到达了系统的安全设计。

4.2 用户登录密码加密算法

本系统在用户登陆模块,使用md5单向加密算法,将用户登陆密码加密,存储于数据库的password字段中。因为加密后的信息是用二进制保存的,即使数据库被人盗取,也不可能知道密码的具体意思。但是有的时候md5加密的二进制数据很容易被解密,从而得到密码原文。在本系统中,在用户注册时,将用户的登录密码通过md5加密后再加上登录密码的下标是奇数的字符存于数据库中(当然你可以使用其他的随机算法),在登录的时候使用同样的机制得到密码进行验证,这样大大提高了系统的安全性。

4.3 Session对象的应用

Session是用户在登录后,在服务器上记录一些信息。Session变量是个有规律的全局变量,当一个Session变量被注册,可以在所有的JSP页面上得到Session变量的值。用Session. setAttribute("variable_name", variable_value)方法可以注册一个Session变量。在所有页面中要想使用已注册的Session变量,就可以由Session. getAttribute("variable_name")方法得到Session变量的值。本系统在用户登录时使用Session对象,用来保存用户名和用户的操作权限。用户在访问一个页面时,在页面的一开始利用Session. getAttribute("variable_name")方法得到Session变量的值,如果用户还没有登录或是会话超期,系统将弹出一个用户登录的界面。如果用户已经登录过,程序就会取得该用户已经注册过的用户名和操作权限,如果用户没有权限使用相关的功能,系统将弹出一个权限不够的提示对话框,本系统使用巧妙的运用Session对象来跟踪用户的痕迹,将一个会话期间用户进行的操作活动记录在里面。同时,使用Session对象可以防止非法用户可能猜测到某个页面的绝对路径,然后在网页浏览器地址栏中直接输入该页面的绝对路径来访问该页面[6-7]。

5 结束语

Java Web开发有两种开发模式:Model1:JSP + JavaBean开发模式和Model2:MVC开发模式。Model1模式在开发中小型项目时具有较大的优势,但有它的不足,如程序的复用度不高。MVC模式实现了业务逻辑、显示逻辑和控制逻辑的分离,适合大规模项目的开发,但开发起来相对于Model1复杂,步骤较多。综合考虑了各个方面,对于本系统我们采用Model1模式进行开发。当系统规模发生变化时,本系统也很容易从Model1转化到Model2。本系统还使用了CSS,Flash,GIF

(下转第40页)

万方数据

版),2006,35(2):18-22.
[4] 李勇,桑艳艳. Web 智能检索中动态相关反馈技术研究[J]. 情报理论与实践,2003,26(2):178-181.
[5] 王斌,谢庆生. Web 教学资源主题检索系统设计与实现[J]. 现代图书情报技术,2006(1):62-65.
[6] David A Grossman, Ophir Frieder. Information Retrieval: Algorithms and Heuristics[M]. Kluwer Academic Publishers, 1998.

Study on Intelligent Search Engine Oriented Model of User Interest Features

ZHANG Ying-jian
(Editorial Department, Journal of Yancheng Institute of Technology, Jiangsu Yancheng 224051, China)

Abstract: Intelligent search engine oriented user interest features were mined through direct and feedback study, and an interest feature-related database was established. User interest feature ascending algorithm was proposed to revise the rights of user interest features automatically. Finally, a case was employed to prove the importance of establishing user interest model.
Keywords: intelligent search engine, user interest feature, feature database

(上接第36页)

动画,Java Script 特效等技术,使得系统有很好的用户界面,给人一个舒适的操作环境。如果数据库使用 Oracle,相信安全性设计过程会更简单,安全性将更高。

参考文献:

[1] 邓子云,张赐. JSP 网络编程从基础到实践[M]. 北京:电子工业出版社,2006.
[2] 余金山,林惠. SQL Server 2000/2005 数据库开发实例入门与提高[M]. 北京:电子工业出版社,2006.
[3] 彭海云, 朱秀丽. 基于 JSP 的高校师生互动平台的构建[J]. 计算机系统应用,2006(10):55-57.
[4] 柳永坡,刘雪梅,赵长海. JSP 应用开发技术[J]. 北京:人民邮电出版社,2005.
[5] 王琴,杨宗凯,吴砥. 基于工作流和 JSP/Servlet 技术的网上项目申报与管理系统设计[J]. 计算机应用研究,2006(12):181-184.
[6] 谢长勇,刘知贵,郑晓红,等. 基于模式2的 JSP 管理信息系统的设计与实现[J]. 计算机应用研究,2006(7):135-137.
[7] 李爱国,邹黎敏,伍俊良. 基于 PHP 信息发布系统实现的新方法[J]. 盐城工学院学报:自然科学版,2008(1):57-61.

Security Design and Implementation of Commodity Marketing System Based on JSP

YANG Jun
(Department of Admission and Employment of Yancheng Institute of Technology, Jiangsu Yancheng 224003, China)

Abstract: This paper aims to describe the feature and superiority of JSP and accomplish commodity marketing system by JSP. The demand analyses and function for the system are given. Especially, we introduce character filter technology, md5 one-way password algorithm, stochastic algorithm, and JSP's session object to achieve security design.
Keywords: JSP; security design; commodity marketing system

万方数据