MVC 架构下网站的设计与实现

刘桃丽,曾志超
(广东海洋大学 数学与计算机学院,广东 湛江 524008)

摘 要:随着科技的高速发展,互联网已经成为了各个部门工作上必不可少的一项工具。针对目前网站设计中普遍存在的扩展性较差、安全性不高、开发难度大以及后期维护困难等问题,提出了一种采用 MVC 架构结合 Java 编程及数据库应用的网站设计方法。MVC 模式是一种先进的 Web 服务设计模式,通过 MVC 架构运用可以优化网站设计。该方法使网站的开发难度得到极大的降低,保证了数据的安全,使网站的安全性大大提高,功能扩展及升级以及后期维护变得更加简单,不仅满足了客户的需求,也是一种先进、安全可靠的网站开发方法。以广东海洋大学科技处网站为例,详细介绍了采用 MVC 框架进行网站开发的关键技术开发过程,尤其是对于网站的安全性如 XSS 和 SQL 注入,做了针对性的预防,从而极大地提高了网站的安全性。

关键词:网站设计;MVC 框架;数据库;网络安全
中图分类号:TP39 **文献标识码**:A **文章编号**:1673-629X(2020)02-0188-04
doi:10.3969/j.issn.1673-629X.2020.02.036

Design and Implementation of Website under MVC Architecture

LIU Tao-li, ZENG Zhi-chao
(School of Mathematics and Computer Science, Guangdong Ocean University, Zhanjiang 524008, China)

Abstract: With the rapid development of science and technology, the Internet has become an indispensable tool in the work of various departments. In view of the existing problems in website design, such as poor extensibility, low security, difficult development and difficult maintenance, we propose a website design method that combines MVC architecture with Java programming and database application. MVC is an advanced Web service design pattern, which can optimize the website design through the application of MVC architecture. This method can greatly reduce the difficulty of website development, ensure the security of data, greatly improve the security of website, and makes function expansion and upgrade and later maintenance easier. It not only can meet the needs of customers, but also be an advanced, safe and reliable website development method. Taking the website of the science and technology department of GuangDong Ocean University as an example, we introduce the key technology and development process of the website development with the MVC framework in detail, especially the targeted prevention of website security such as XSS and SQL injection, thus greatly improving the safety of website.

Key words: website design; MVC framework; database; network security

0 引 言

随着科技的高速发展,互联网已经成为了各个部门工作上必不可少的一项工具。各类机构内部的各项工作的提出、组织、记录、总结和展示,都可以通过网站来实现。网站全面包含了科技成果的发表和展示,网络,可以有效地对工作中必要的数据进行记录和查询,提高工作效率。因此,网站的设计和开发变得尤为重要,不仅要满足客户的需求,保证数据的安全,并且应该具有功能可扩展性、升级便利以及便利的后期系统维护。文中以广东海洋大学科技处网站为例,采用 MVC 架构及相关技术进行开发,很好地解决了以上问题。

1 MVC 框架简介

MVC,即 Model View Controller,是模型(model)-视图(view)-控制器(controller)的缩写[1-2],是一种经典的软件开发设计模型。这种设计模式将业务逻辑、数据、界面显示分离开来,将业务逻辑聚集到一个部件

收稿日期:2019-02-18 **修回日期**:2019-06-20 **网络出版时间**:2019-11-07
基金项目:广东省教育教学改革项目(2016040604);2016 广东海洋大学大学生创新创业项目(CXXL20161312)
作者简介:刘桃丽(1981-),女,硕士研究生,讲师,从事软件工程专业的教学与研究。
网络出版地址:http://kns.cnki.net/kcms/detail/61.1450.TP.20191107.0908.018.html

里面,这样的设计模式,不需要重写业务逻辑,就可以轻松改进和个性化定制界面及用户交互[3]。同时 MVC 框架具有耦合性低、重写性高、生命周期成本低、可维护性低、有利于软件工程化管理等特点。使用 MVC 设计模式,主要的目的是使模型和视图实现分离,里边各类专业人员各司其职,从而大大提升开发效率[4]。

2　MVC 框架下网站的设计过程——以广东海洋大学科技处网站为例

2.1　系统的整体架构设计

广东海洋大学科技处根据 MVC 三层架构的模式进行架构设计。表示层,即用户浏览器前端,主要用途是将用户所需要的数据尽可能简洁美观地呈现出来;业务逻辑层,主要是对用户的请求进行响应,并根据用户需求对数据库进行相应的增删改查操作,本网站的业务逻辑层主要提供了科技成果、科技动态、科技新闻、科研成果、组织机构、知识产权、学术活动和办事指南等类型文章的相关接口,以及其他附加相关业务接口;数据持久层,即数据库,主要功能是将用户产生的大量数据进行有规律的存储,并提供高效的增删改查功能。

2.2　系统的整体模块设计

广东海洋大学科技处系统主要分为 7 大模块:图片管理模块、通知公告管理模块、文件模块、搜索模块、用户模块、科研平台模块、文章信息模块。图片管理模块主要功能是管理员对首页轮播图片和成果展示版面图片的更替,通知公告模块主要功能是对科技处必要公告的发布和展示,文件模块功能为网站的文件上传和下载等管理,搜索模块为系统提供整体的搜索功能,用户模块主要是科技处成员的登录注册以及超级管理员的账户增删改查管理,科研平台模块为管理员提供平台机构的增删改查管理,文章信息模块则通过一个编辑器,提供了方便的文章发布途径。各模块及其功能如图 1 所示。

2.3　系统的主要业务流程

广东海洋大学科技处网站面向不同用户时,主要业务流程也各不相同。对于普通的网站使用用户而言,业务较为简单,主要为浏览科技处发布的相关通知与新闻与下载办事所需的各类文档、模板或是年度总结文档。科技处网站的下载业务分为年报下载与下载专区文件下载。下载年报时,可以自主选择下载特定年度的年报;而下载专区文件可在首页查看最新可下载文件,并且还可进入下载专区,查看并下载各个分区下的文件。科技处网站还设有全站搜索功能,用户可以在搜索框中输入关键字,进行全站搜索,当存在相关内容时,会分页展示所有相关内容。除此之外,用户还可以通过导航栏的入口查看部门职能说明、科研平台介绍等内容。

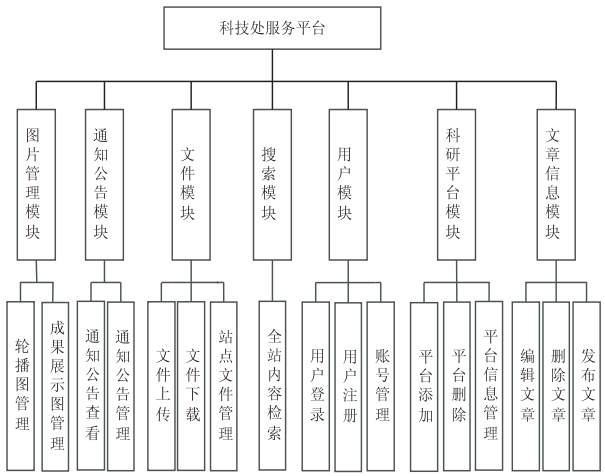

图 1　广东海洋大学科技处系统模块功能

科技处网站的管理人员需要管理站点时,首先需要通过首页入口登录后台管理系统,进入后台后,可以对各个分类的文章进行添加、修改、删除与发布操作。同时,管理员登录科技处网站后台管理系统还可对首页轮播图进行管理,修改轮播图展示图片与指向链接;添加、修改科技成果板块的展示图;上传、删除年报,下载专区的文件;设置首页漂浮盒标题与指向内容等。系统的业务流程图有很多,最为简单的为用户登录流程,也有较为复杂的业务,比如用户文件的发布、上传和下载等。

2.4　系统数据库设计

该系统使用 MySQL[5] 数据库来管理用户数据。MySQL 是一种关系数据库管理系统,该数据库系统根据数据之间的关系,灵活地将不同的数据存放在不同的数据表格中,数据库创建的表有很多,主要包括学术年报表、通知表、校园文章表、其他文章表以及相关的政策法规、科研平台表等。

2.5　安全性问题

网站的安全性问题至关重要,涉及到网站能否正常运行,数据是否安全,内容是否容易被非法入侵者篡改,服务器是否容易被控制和攻击等方面[6-7]。因此安全性问题是每一个成熟的系统都比较重视的问题[8]。该系统主要的安全性问题是防止 XSS 和 SQL 注入。

(1)XSS 安全性问题。

XSS 指的是跨脚本攻击[9],攻击者向存在 XSS 漏洞的网站中注入恶意 HTML 代码,当客户打开该网页时,会自动执行此恶意代码,从而导致一系列的问题,比如强行定向跳转到指定网站,恶意破坏网页,盗取用户信息等[10]。这是网站中最常遇见的安全性问题。

由于跨脚本攻击是针对客户端的攻击方式,这种被动式的攻击最容易被开发者忽视,因此也成为最常见的系统安全漏洞。

针对这类问题,该系统对所有的注入可能进行了严格的筛选和过滤,对用户的一些攻击性语句进行转义,及将用户输入的代码转换成可执行代码进行存储,而在展示的时候将可执行代码转变成文本信息,从而起到保护隔离的作用,避免可执行代码直接暴露在前台页面,大大提高网页的安全性。

(2)SQL 数据库安全性问题。

在使用 SQL 数据库系统时,最常见的问题就是注入性问题[11]。所谓的注入性问题,就是非法入侵者使用某些恶意的数据库命令注入到数据库的引擎中,对服务器进行欺骗性操作,从而获取数据库的相关表格的查询权限。此类问题最容易引起的后果就是数据泄露,如重要的用户名和密码的表单,是被攻击的重灾区。

为了解决此类问题,该系统采用的处理方法有两种,一是使用参数化的 SQL 命令或者只是使用存储过程进行数据的查询与存取,舍弃动态拼装命令[12];二是对用户的查询输入进行校验和转换。通过这两种方法可以在很大程度上解决数据库的注入性问题。

2.6 系统的关键技术实现

(1)ueditor 图片上传文件下载。

该系统使用的一个核心插件是百度提供的 ueditor 编辑器[13],它功能非常强大,基本上可以满足系统的所有需求。但是在使用该插件的过程中,发现它也还是有缺陷的。当用户上传一张很大的图片时,它默认显示原图片大小,因此最后的效果就是占满了整个屏幕。解决该问题的方案便是查询源码,给该图片设置宽度,高度自适应。但是这样又会有一个问题,不管是大图还是小图,最后都使用了统一设置的宽度。ueditor 编辑器提供了两个上传图片的按钮,一个是 simpleupload 单图上传,一个是 insertimage 多图上传。因此采取折中的做法,就是当图片比较大时,用 simpleupload 按钮来上传,最后效果便是给设定的宽度;当图片是小图或者是想显示原图大小时,就用 insertimage 按钮来上传。

另一个问题就是在 ueditor 添加附件后,如果是 .txt或者 .pdf 等格式文件,点击该附件下载时,浏览器直接解析了。查看源码发现,只是用了一个 a 标签进行简单的资源链接而已。因此,通过修改源码,用户点击附件之后不会被浏览器直接解析,而是会通知浏览器进行下载。

(2)同张表多类型数据分页加载。

该系统在很多地方都用了分页加载技术,但该系统中的分页加载技术跟以往很多系统不同。以前系统进行分页加载的做法是直接拿到前端传过来的页码,使用 limit 就可以直接从数据库中查出来。但在该系统中,由于数据库中多数表的设计用了一个 type 字段,该字段划分了不同类型的数据资源,而且它们在数据库中顺序错综复杂。当要对某一种 type 类型数据进行分页加载时,比如每页加载 20 条数据时,每一次分页加载的数据,需要记录最后一条数据的 id,将最后一条数据的 id 作为下一次分页的起点。当然用 id 作为一个定位还有一个好处就是,id 是主键,是建立了索引的,因此大大优化了系统的性能[14]。

(3)根据 ip 进行内外网管制。

在系统基本开发完成的时候,客户新增需求需要对内外网进行管制。客户要求有些内容只能是校园网才能查看和下载。为了实现该需求,有两种方案,一种是修改数据库表,给每个表添加一个字段,用于区分外网是否可用查看或下载。但是这种方案有点不太理想,因为修改数据库表的话,意味着很多东西都要修改,而大规模的修改对于开发者无疑是一个灾难。因此采取了第二种方案,即新增一个表,用于存放校园网能查看和下载的资源。毕竟大部分资源外网都是能查看和下载的,只有少部分是只有校园网用户才能查看的。基于这样的思想,新增了一个表,因此在前端返回数据时,根据用户的 ip,如果是外网,则需要过滤校园表中的数据,如果是内网,则不需要过滤校园表中的数据。另外,为了提高系统的响应性能,利用了数据缓存技术[14]和数据监听技术[15],不仅减少了数据库操作带来的系统性能损耗,同时也大大提高了系统的响应性能。

2.7 系统前端页面简要展示

主界面由“部门首页、组织机构、政策法规、科研平台、科技成果、知识产权、学术活动、学年报告、办事指南”9 个选项卡构成,如图 2 所示。首页主要用途是对外展示广东海洋大学科技处的科研成果、科研资料以及最新科技动态等,还包括以下科技处内部的通知、管理类文件的查看和下载。

科技处的后台管理员界面需要管理员以管理员身份登录后才有足够的操作权限。后台管理员可发布“自然科学类,人文科学类,成果与知识产权类”的文章,发布后,系统会根据不同的类型到不同的模块上展示。管理员可以发布学术年报、链接其他网站的科技动态等功能。

2.8 系统使用效果

系统测试是一款应用软件上架前重要的一环。该网站通过白盒测试、黑盒测试以及半年的试用期后,于 2017 年 3 月份正式上线使用,系统上线至今已经两

年,期间除因为需求问题对系统进行相应的扩展之外,未出现任何安全事故以及其他使用上的问题,而且系统运行流畅,使用效果良好,性能完全达到了客户要求。

图 2　科技处网站主界面

3　结束语

广东海洋大学网站是一个高效的工作网站,其涉及 MVC 设计模式的开发,使得系统具有很好的维护效率和质量。为了加强网站的安全性能,尤其是针对数据安全,特别对 XSS 和 SQL 注入问题进行了防范,确保了数据安全。系统采用改造后的 ueditor 编辑器对图片上传和下载进行处理,并采用数据表格分页加载技术,针对校园网使用要求,对内网和外网给予不同的访问权限,对外网访问权限进行了相应的限制。以上种种措施,大大提高了系统的响应速度和数据的安全性。经过半年的测试及两年的使用,结果表明该网站运行稳定、数据安全、扩展方便、维护便利。

参考文献:

[1] 贾顺贺,陈建飞,陈古运,等. 基于 MVC 架构的个人健康信息管理系统设计与实现[J]. 计算机应用与软件,2018,35(3):43-48.

[2] 王玉英. 基于 JSP 的 MySQL 数据库访问技术[J]. 现代计算机,2010(14):67-70.

[3] 王志刚. MySQL 高效编程[M]. 北京:人民邮电出版社,2012.

[4] 潘　杰,周传生. 基于 jQuery 框架的 Web 研究与实现[J]. 沈阳师范大学学报:自然科学版,2015,33(1):96-99.

[5] 张家前,项吴曙,刘春兰,等. 基于 MVC 模式的油罐车多参数远程监测系统的设计[J]. 工业控制计算机. 2018,31(5):127-128.

[6] 林子雨,邹　权,赖永炫,等. 关系数据库中的关键词查询结果动态优化[J]. 软件学报,2014,25(3):528-546.

[7] 林信良. Spring4.0 技术手册[M]. 北京:电子工业出版社,2015.

[8] 孙卫琴,李洪成. Tomcat 与 Java Web 开发技术详解[M]. 北京:电子工业出版社,2004.

[9] APARNA S,KUMAR V S. Speech recognition using backoff N-Gram modelling in Android application[J]. International Journal of Computer Science and Mobile Computing,2014,3(1):501-507.

[10] 盖索林. Google Android 开发入门指南[M]. 第 2 版. 北京:人民邮电出版社,2009.

[11] 刘胜前,陈立定. 基于 Android 平台的车辆导航系统设计与实现[J]. 自动化与仪表,2012,27(4):1-4.

[12] PANDITA R,XIAO X,YANG W,et al. WHYPER:towards automation risk assessment of mobile applications[C]//Proceedings of the 22th USENIX conference on security. Washington D. C:USENIX Association Berkeley,2013:527-542.

[13] WAN J,WANG J,XIE C,et al. S2RAID:parallel RAID architecture for fast data recovery[J]. IEEE Transactions on Parallel and Distributed Systems,2014,25(6):1638-1647.

[14] LIU F,PAN W,XIE T,et al. PDB:a reliability-driven data reconstruction strategy based on popular data backup for RAID4 SSD arrays[M]//Algorithms and architectures for parallel processing. [s. l.]:[s. n.],2013:87-100.

[15] NIE Fengming, XU Feng, QI Rongzhi. SAML-based single sign-on for legacy system automation and logistics (ICAL)[C]//2012 IEEE international conference on automation and logistics. Zhengzhou:IEEE,2012:470-473.