河南工業大學

毕业设计(论文)
开题报告

题　　目: 基于 SSM 的客户信息管理系统的设计与实现

院系名称： 信息科学与工程学院 专业班级： 软件工程 1503

学生姓名： 王进 学　　号 201516920522

指导教师： 程凤娟 教师职称： 副教授

2019 年 3 月 5 日

开题报告填写要求

1．开题报告（含“文献综述”）作为毕业设计（论文）答辩委员会对学生答辩资格审查的依据材料之一。此报告应在指导教师指导下，由学生在毕业设计（论文）工作前期内完成，经指导教师签署意见及所在专业审查后生效。

2．开题报告内容必须用黑墨水笔工整书写或按教务处统一设计的电子文档标准格式（可从教务处网页上下载）打印，禁止打印在其它纸上后剪贴，完成后应及时交给指导教师签署意见。

3．“文献综述”应按论文的格式成文，并直接书写（或打印）在本开题报告第一栏目内,学生写文献综述的参考文献应不少于15篇，其中英文文献不少于2篇。

4．有关年月日等日期的填写，应当按照国标GB/T 7408—94《数据元和交换格式、信息交换、日期和时间表示法》规定的要求，一律用阿拉伯数字书写。如“2017年11月20日”或“2017-11-20”。

毕业设计（论文）开题报告

1．结合毕业设计（论文）课题情况，根据所查阅的文献资料，每人撰写不少于2000字的文献综述：

文 献 综 述

1、选题背景

网络是信息传输、接收、共享的虚拟平台，通过它把世界上所有的信息联系在一起，从而实现资源共享。它是我们学习、工作、生活、科研等都离不开的一个重要工具。

随着时代的发展，计算机已经完全融入了我们的生活，在我们的生活中计算机是非常重要的。计算机能够带来信息革命，大数据爆炸的时代，计算机给我们带来了非常多好处的同时，也有很多的风险存在。有“熊猫烧香”软件方面的风险，也有“911”大爆炸导致的恐怖分子风险，也有技术人员没有做好抵抗天灾带来的硬件损毁的风险等等。这些都对企业以及个人信息安全带来了更多的风险，也对信息安全提出了更高的要求。

2、行业安全现状

网站：

1)注入攻击检测Web网站是否存在诸如SQL注入、SSI注入、Ldap注入、Xpath注入等漏洞，如果存在该漏洞，攻击者对注入点进行注入攻击，可轻易获得网站的后台管理权限，甚至网站服务器的管理权限。

2) XSS跨站脚本检测Web网站是否存在XSS跨站脚本漏洞，如果存在该漏洞，网站可能遭受Cookie欺骗、网页挂马等攻击。

3)网页挂马检测Web网站是否被黑客或恶意攻击者非法植入了木马程序。

4)缓冲区溢出检测Web网站服务器和服务器软件，是否存在缓冲区溢出漏洞，如果存在，攻击者可通过此漏洞，获得网站或服务器的管理权限。

5)上传漏洞检测Web网站的上传功能是否存在上传漏洞，如果存在此漏洞，攻击者可直接利用该漏洞上传木马获得WebShell。

6)源代码泄露检测Web网络是否存在源代码泄露漏洞，如果存在此漏洞，攻击者可直接下载网站的源代码。

7)隐藏目录泄露检测Web网站的某些隐藏目录是否存在泄露漏洞,如果存在此漏洞，

攻击者可了解网站的全部结构。

8)数据库泄露检测 Web 网站是否在数据库泄露的漏洞，如果存在此漏洞，攻击者通过暴库等方式，可以非法下载网站数据库。

9)弱口令检测 Web 网站的后台管理用户，以及前台用户，是否存在使用弱口令的情况。

10)管理地址泄露检测 Web 网站是否存在管理地址泄露功能，如果存在此漏洞，攻击者可轻易获得网站的后台管理地址。

网络：

1)结构安全与网段划分

网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；根据机构业务的特点，在满足业务高峰期需要的基础上，合理设计网络带宽；

2)网络访问控制

不允许数据带通用协议通过。

3)拨号访问控制

不开放远程拨号访问功能（如远程拨号用户或移动 VPN 用户）。

4)网络安全审计

记录网络设备的运行状况、网络流量、用户行为等事件的日期和时间、用户、事件类型、事件是否成功，及其他与审计相关的信息；

5)边界完整性检查

能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断；能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

6)网络入侵防范

在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫攻击等入侵事件的发生；当检测到入侵事件时，记录入侵源 IP、攻击类型、攻击目的、攻击时间等，并在发生严重入侵事件时提供报警（如可采取屏幕实时提示、E-mail 告警、声音告警等几种方式）及自动采取相应动作。

7)恶意代码防范

在网络边界处对恶意代码进行检测和清除；维护恶意代码库的升级和检测系统的更新。

8)网络设备防护

对登录网络设备的用户进行身份鉴别；对网络设备的管理员登录地址进行限制；主要网络设备对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别

主机：

1)身份鉴别

对登录操作系统和数据库系统的用户进行身份标识和鉴别；

2)自主访问控制

依据安全策略控制主体对客体的访问。

3)强制访问控制

应对重要信息资源和访问重要信息资源的所有主体设置敏感标记；强制访问控制的覆盖范围应包括与重要信息资源直接相关的所有主体、客体及它们之间的操作；强制访问控制的粒度应达到主体为用户级，客体为文件、数据库表/记录、字段级。

4)可信路径

在系统对用户进行身份鉴别时，系统与用户之间能够建立一条安全的信息传输路径。

5)安全审计

审计范围覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；审计内容包括系统内重要的安全相关事件。

6)剩余信息保护

保证操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；确保系统内的文件、目录和数据库记录等资源所在的存储空间

能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；能够对重要程序完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施；操作系统遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。

7)恶意代码防范

安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；主机防恶意代码产品具有与网络防恶意代码产品不同的恶意代码库；支持防恶意代码的统一管理。

8)资源控制

通过设定终端接入方式、网络地址范围等条件限制终端登录；根据安全策略设置登录终端的操作超时锁定；对重要服务器进行监视，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况；限制单个用户对系统资源的最大或最小使用限度；当系统的服务水平降低到预先规定的最小值时，能检测和报警。

数据库：

主流数据库的自身漏洞逐步暴露，数量庞大；仅 CVE 公布的 Oracle 漏洞数已达 1100 多个；数据库漏扫可以检测出数据库的 DBMS 漏洞、缺省配置、权限提升漏洞、缓冲区

溢出、补丁未升级等自身漏洞。

3、研究意义

随着计算机技术的飞速发展，计算机信息安全问题越来越受关注。无论是软件方面的信息安全问题，还是硬件方面的信息安全问题，掌握必要的信息安全管理和安全防范技术是非常必要的。掌握计算机信息安全的基本原理和当今流行的信息安全设置、安全漏洞、防火墙的策略与实现、黑客原理与防范，以便能够胜任信息系统的实现、运行、管理与维护等相关的工作。

4、主要研究内容

本选题的目的是开发一个基于 SSM 的客户信息管理系统。系统功能有系统管理、员工管理、客户管理、订单管理等主要功能功能。员工信息管理根据员工等级进行查看客户的相关或一部分信息、修改信息、删除信息、添加信息四个子功能；员工授权可以对员工进行等级授权；系统管理包括最高管理员对系统的员工信息的增加功能、删除功能、修改功能、查询功能，对客户的增加功能、删除功能、修改功能、查询功能。

5、研究方法

本次毕业设计采用 Orance[1]数据库，数据后台逻辑采用 SpringBoot[2]，数据持久化采用 Mybatis[3]、前端采用 BootStrap[4]，使用 JavaScript[5]]进行数据的异步交互。

6、研究条件为完成课题已具备和所需的条件

已具备 java 基础知识以及数据库基础知识，还需要学习 JavaScript 知识。

7、研究步骤

具体的需求分析、合理的开发步骤、技术、编码、测试、优化。

参考文献：

[1] 唐汉明. 深入浅出 MySQL[M]. 北京: 人民邮电出版社. 2014: 88-126

[2] Craig Walls. Spring Boot in Action[M]. 北京: 人民邮电出版社. 2016: 238 -262

[3] 黄艳秀.基于 mybatis 的面向数据库自动生成技术[M]. 河南: 河南科技大学 2014: 88-125

[4] 徐涛.深入理解 Bootstrap[M]. 北京: 机械工业出版社.2014: 155-182

[5] 陆凌牛. HTML 与 CSS3 权威指南[M]. 北京: 机械工业出版社. 2015: 382-429

[6] 刘继承.JAVA 程序设计及实验[M]. 北京: 清华大学出版社

[7] 明日科技. JavaScript[M]. 北京: 清华大学出版社. 2017: 127-146

[8] Bruce Eckel. Thinking in Java[M]. 美国: Prentice Hall. 2006

[9] 周志明. 深入理解 JAVA 虚拟机[M]. 北京: 机械工业出版社. 2013

[10] 杨冠宝. 码出高效-Java 开发手册[M]. 北京: 电子工业出版社. 2018

[11] Paul DuBois.MySQL 技术内幕[M]. 北京: 人民邮电出版社. 2015

[12] 李刚. 疯狂 Java 讲义[M]. 北京: 电子工业出版社. 2019

[13] 储久良. Web 前端技术[M]. 北京: 清华大学出版社. 2018

[14] 许令波. 深入分析 Java Web 技术内幕[M]. 北京: 电子工业出版社. 2014

[15] 陈强.精通 Java 开发技术[M]. 北京: 清华大学出版社.2014

[16] Kathy Sierra. Head First Java[M]. 北京: 中国电力出版社. 2008

[17] 徐述.数据库管理系统概论[M]. 北京: 清华大学出版社,2018

[18] Dalwoo Nam.Business analytics use in CRM: A nomological net from IT competence to CRM performance[J].Journal of Business Research,2019: 233-245.

[19] Thomas R.The Future of CRM[J].Crew Resource Management (Third Edition),2019: 581-585.

[20] IlariaDalla Pozza.Implementation effects in the relationship between CRM and its performance[J].Journal of Business Research,2018: 391-403

毕业设计（论文）开题报告

２．本课题要研究或解决的问题和拟采用的研究手段（途径）：

课题目标

①认识并了解网络信息安全的知识，并采用对应方法去尽量保证信息的安全。

②学习 Java 中 SpringBoot+Mybatis。

③学习 JavaScript。

④学习 Orance 数据库。

研究手段

1、通过网络查阅相关知识来了解网络信息安全，并通过比较全面的方案来保证信息安全，例如做到开启防火墙、网络安全隔离、安全路由器、虚拟专用网、安全服务器、入侵检测系统、物理防灾、数据备份等操作来尽可能的保证信息的安全。

2、学习加密技术，对代码加密，尽可能完成软件方面安全性的要求。

毕业设计（论文）开题报告

指导教师意见：

1．对“文献综述”的评语：

文献综述表明该生查阅了与客户信息安全管理相关的文献资料，掌握了课题研究的相关基础知识，理解了本课题的选题背景和研究目标，理清了课题相关的研究现状和发展趋势，分析了存在的问题及初步解决办法。综述较为完整，有一定见解，同意开题。

2．对本课题的深度、广度及工作量的意见和对设计（论文）结果的预测：

课题结合 Spring+SpringBoot+Mybatis 框架和 oracle 数据库技术，运用 Java 语言和 Eclipse 环境，设计和实现一个基于 B/S 架构的客户信息安全管理系统。课题难度合适，工作量适中，涉及软件开发所需的大部分知识和技能，广度和深度符合本科毕业设计要求，设计结果具有一定的应用价值。通过课题的实施可以使学生得到比较全面的软件项目开发训练，培养解决软件工程领域复杂工程问题的能力，预计该生能够按时完成毕业设计。

指导教师签字：_____

年　月　日

系（教研室）审核意见：

负责人（签章）：_____

年　月　日