《信息系统安全》课程设计

InfoSec项目要求

华南理工大学 软件学院

2020

总体目标：在约定部署环境及应用环境下，增强一个Java EE Web应用系统（简称InfoSec）的整体安全性。

InfoSec简述：

技术栈：

1. Java EE动态Web应用，底层为Java Servlet技术。
2. 具体开发时，并不直接进行servlet编程，而是使用Spring MVC技术来实现代码的解耦合。其中一个层次的解耦和使得业务代码UserContorller与Servlet API无关，便于代码进行单元测试与移植。
3. 系统使用面向对象的数据访问技术（Object Relational Mapping，简称ORM），具体为Mybatis。
4. 请了解控制反转（Inversion of Control, 简称IOC）与依赖注入（Dependency Injection，简称DI）基本原理。系统利用Spring Bean技术来管理对象实例的管理，在系统初始化时，Spring IOC容器根据配置文件，初始化并注册相应Bean实例。业务Bean，如UserContorller，使用注解+自动扫描方式实现，无需在xml配置文件中手写代码配置。

数据上，InfoSec非常简单，仅存在一个数据库表user，用于表示系统用户。创建数据库表的sql文件在/infosec/sql/中；初始数据存在两个用户，分别为mic和mulan。

业务上，InfoSec非常简单，仅有两个业务。一个是获取系统用户列表，另外一个是查看用户详细信息。

部署与访问：

1. 使用Java 6及以上版本
2. 部署在Tomcat 8.0 版本的Web容器中，端口使用80
3. 数据库系统使用MySql 5版本; 记得修改database.properties中的链接参数；
4. 运行主机的操作系统为Windows 2008 Server或者CentOS 7
5. 部署在内网，使用IP为192.168.0.10/24（或者其他私有IP地址）
6. 要求InfoSec应用内网与公网均可访问，在考虑安全前提下，尽可能考虑性能。

项目文件：eclipse Web工程项目，使用eclipse IDE进行开发。请了解相关技术后，也读相关源文件后再进行开发！

具体要求：先分析系统可能存在的威胁，然后进行如下多个方面的增强。

1. 如何实现通信安全？请使用TLS/SSL传输层安全机制实现。
2. 如何实现业务安全？要求使用Spring Security实现！
   1. 实现安全用户认证（用户名与密码方式）非系统认证用户，仅可访问主页”index.jsp”和登陆页面”/login.jsp”等静态页面。
   2. 实现基于角色的访问控制策略：仅管理员角色（ROLE\_ADMIN）可访问“获取系统用户列表“业务，并可访问” 查看用户详细信息“业务，查看任何用户信息；其他认证用户，均可访问” 查看用户详细信息“业务，但是仅能查看本用户的信息。
3. 如何使用数字证书进行用户验证（替代用户名/密码机制），分析该机制的安全性，可用性等（依赖Spring Security实现，可以采用其他方案）
4. 服务器是如何实现认证的？考虑到用户因素，该机制安全性如何？
5. 数据库系统安全？如何安全配置MySql5数据库系统等
6. 操作系统安全？防火墙，默认开启服务等多个方面。
7. 你所能考虑的其他方面?比如软件开发管理，软件测试等方面，提供系统的可靠性。

分组：4~5人一组，分工合作，小组交一份报告，必须注明个人具体完成的地内容，介绍总体想法，和自己所做的工作。

请使用课程设计论文模板！

附：如果你发现不清楚的，及时在QQ群中询问，我统一做出回复。