**品优购电商系统开发**

**第5章**

**安全框架与商家入驻审核**

传智播客.黑马程序员

# 1.Spring Security框架入门

## 1.1 Spring Security简介

Spring Security是一个能够为基于Spring的企业应用系统提供声明式的安全访问控制解决方案的安全框架。它提供了一组可以在Spring应用上下文中配置的Bean，充分利用了Spring IoC，DI（控制反转Inversion of Control ,DI:Dependency Injection 依赖注入）和AOP（面向切面编程）功能，为应用系统提供声明式的安全访问控制功能，减少了为企业系统安全控制编写大量重复代码的工作。

## 1.2 Spring Security入门小Demo

### 1.2.1最简单Demo

（1）创建工程spring-demo-security ,pom.xml内容

|  |
| --- |
| <properties>  <spring.version>4.2.4.RELEASE</spring.version>  </properties>  <dependencies>  <dependency>  <groupId>org.springframework</groupId>  <artifactId>spring-core</artifactId>  <version>${spring.version}</version>  </dependency>  <dependency>  <groupId>org.springframework</groupId>  <artifactId>spring-web</artifactId>  <version>${spring.version}</version>  </dependency>  <dependency>  <groupId>org.springframework</groupId>  <artifactId>spring-webmvc</artifactId>  <version>${spring.version}</version>  </dependency>  <dependency>  <groupId>org.springframework</groupId>  <artifactId>spring-context-support</artifactId>  <version>${spring.version}</version>  </dependency>  <dependency>  <groupId>org.springframework</groupId>  <artifactId>spring-test</artifactId>  <version>${spring.version}</version>  </dependency>  <dependency>  <groupId>org.springframework</groupId>  <artifactId>spring-jdbc</artifactId>  <version>${spring.version}</version>  </dependency>  <dependency>  <groupId>org.springframework.security</groupId>  <artifactId>spring-security-web</artifactId>  <version>4.1.0.RELEASE</version>  </dependency>  <dependency>  <groupId>org.springframework.security</groupId>  <artifactId>spring-security-config</artifactId>  <version>4.1.0.RELEASE</version>  </dependency>  <dependency>  <groupId>javax.servlet</groupId>  <artifactId>servlet-api</artifactId>  <version>2.5</version>  <scope>provided</scope>  </dependency>  </dependencies>  <build>  <plugins>  <!-- java编译插件 -->  <plugin>  <groupId>org.apache.maven.plugins</groupId>  <artifactId>maven-compiler-plugin</artifactId>  <version>3.2</version>  <configuration>  <source>1.7</source>  <target>1.7</target>  <encoding>UTF-8</encoding>  </configuration>  </plugin>  <plugin>  <groupId>org.apache.tomcat.maven</groupId>  <artifactId>tomcat7-maven-plugin</artifactId>  <configuration>  <!-- 指定端口 -->  <port>8083</port>  <!-- 请求路径 -->  <path>/</path>  </configuration>  </plugin>  </plugins>  </build>  </project> |

（2）创建web.xml

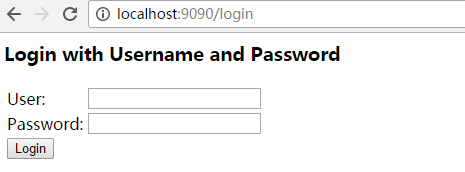
|  |
| --- |
| <?xml version=*"1.0"* encoding=*"UTF-8"*?>  <web-app xmlns:xsi=*"http://www.w3.org/2001/XMLSchema-instance"*  xmlns=*"http://java.sun.com/xml/ns/javaee"*  xsi:schemaLocation=*"http://java.sun.com/xml/ns/javaee http://java.sun.com/xml/ns/javaee/web-app\_2\_5.xsd"*  version=*"2.5"*>  <context-param>  <param-name>contextConfigLocation</param-name>  <param-value>classpath:spring-security.xml</param-value>  </context-param>  <listener>  <listener-class>  org.springframework.web.context.ContextLoaderListener  </listener-class>  </listener>  <filter>  <filter-name>springSecurityFilterChain</filter-name> <filter-class>org.springframework.web.filter.DelegatingFilterProxy</filter-class>  </filter>  <filter-mapping>  <filter-name>springSecurityFilterChain</filter-name>  <url-pattern>/\*</url-pattern>  </filter-mapping>  </web-app> |

（3）创建index.html 内容略

（4）创建spring 配置文件spring-security.xml

|  |
| --- |
| <?xml version=*"1.0"* encoding=*"UTF-8"*?>  <beans:beans xmlns=*"http://www.springframework.org/schema/security"*  xmlns:beans=*"http://www.springframework.org/schema/beans"* xmlns:xsi=*"http://www.w3.org/2001/XMLSchema-instance"*  xsi:schemaLocation=*"http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-beans.xsd*  *http://www.springframework.org/schema/security http://www.springframework.org/schema/security/spring-security.xsd"*>  <!-- 页面拦截规则 -->  <http use-expressions=*"false"*>  <intercept-url pattern=*"/\*\*"* access=*"ROLE\_USER"* />  <form-login/>  </http>  <!-- 认证管理器 -->  <authentication-manager>  <authentication-provider>  <user-service>  <user name=*"admin"* password=*"123456"* authorities=*"ROLE\_USER"*/>  </user-service>  </authentication-provider>  </authentication-manager>  </beans:beans> |

此案例我们没有登录页，而是使用了系统自动生成的登陆页，效果如下：



配置说明：

intercept-url 表示拦截页面

/\* 表示的是该目录下的资源，只包括本级目录不包括下级目录

/\*\* 表示的是该目录以及该目录下所有级别子目录的资源

form-login 为开启表单登陆

use-expressions 为是否使用 Spring 表达式语言（ SpEL ），默认为true ,如果开启，则拦截的配置应该写成以下形式

|  |
| --- |
| <intercept-url pattern=*"/\*\*"* access=*"hasRole('ROLE\_USER')"* /> |

### 1.2.2用户自定义登录页

实际开发中，我们不可能使用系统生成的登录页，而是使用我们自己的登录页。

（1）构建登陆页：

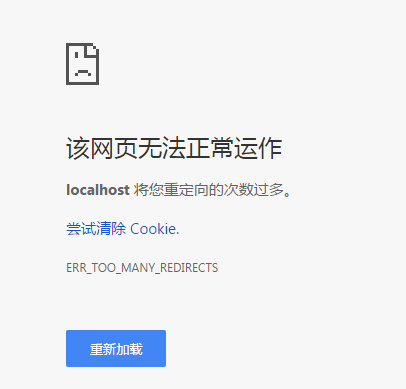
|  |
| --- |
| <!DOCTYPE html>  <html>  <head>  <meta http-equiv=*"Content-Type"* content=*"text/html; charset=UTF-8"*>  <title>登陆</title>  </head>  <body>  <!-- springSecurityDemo为项目名称 -->  <form action=*'/login'* method=*'POST'*>  <table>  <tr>  <td>用户名:</td>  <td><input type=*'text'* name=*'username'* value=*''*></td>  </tr>  <tr>  <td>密码:</td>  <td><input type=*'password'* name=*'password'* /></td>  </tr>  <tr>  <td colspan=*'2'*><input name=*"submit"* type=*"submit"*  value=*"登陆"* /></td>  </tr>  </table>  </form>  </body>  </html> |

1. 构建登陆失败页 error.html（内容略）

（3）修改 spring 配置文件spring-security.xml

|  |
| --- |
| <?xml version=*"1.0"* encoding=*"UTF-8"*?>  <beans:beans xmlns=*"http://www.springframework.org/schema/security"*  xmlns:beans=*"http://www.springframework.org/schema/beans"* xmlns:xsi=*"http://www.w3.org/2001/XMLSchema-instance"*  xsi:schemaLocation=*"http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-beans.xsd*  *http://www.springframework.org/schema/security http://www.springframework.org/schema/security/spring-security.xsd"*>  <!-- 以下页面不被拦截 -->  <http pattern=*"/login.html"* security=*"none"*></http>  <!-- 页面拦截规则 -->  <http use-expressions=*"false"*>  <intercept-url pattern=*"/\*"* access=*"ROLE\_USER"* />  <form-login login-page=*"/login.html"* default-target-url=*"/index.html"* authentication-failure-url=*"/login\_error.html"*/>  <csrf disabled=*"true"*/>  </http>    <!-- 认证管理器 -->  <authentication-manager>  <authentication-provider>  <user-service>  <user name=*"admin"* password=*"123456"* authorities=*"ROLE\_USER"*/>  </user-service>  </authentication-provider>  </authentication-manager>  </beans:beans> |

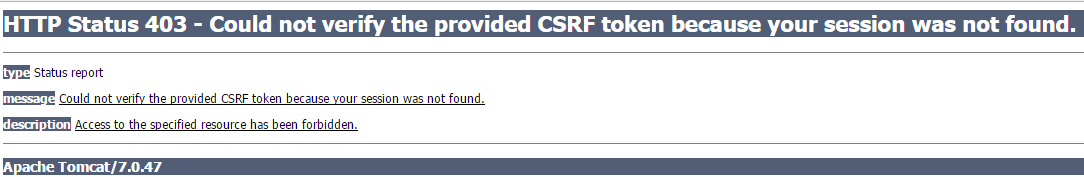
security="none" 设置此资源不被拦截.   
如果你没有设置登录页security="none" ，将会出现以下错误



因为登录页会被反复重定向。

login-page：指定登录页面。  
authentication-failure-url：指定了身份验证失败时跳转到的页面。  
default-target-url：指定了成功进行身份验证和授权后默认呈现给用户的页面。

csrf disabled="true" 关闭csrf ,如果不加会出现错误 SpringSecurity安全自带



CSRF（Cross-site request forgery）跨站请求伪造，也被称为“One Click Attack”或者Session Riding，通常缩写为CSRF或者XSRF，是一种对网站的恶意利用。

# 2.运营商系统登录与安全控制

## 2.1需求分析

完成运营商登陆功能



## 2.2登陆功能的实现

### 2.2.1配置文件

（1）修改web.xml

|  |
| --- |
| <context-param>  <param-name>contextConfigLocation</param-name>  <param-value>classpath:spring/spring-\*.xml</param-value>  </context-param>  <listener>  <listener-class>  org.springframework.web.context.ContextLoaderListener  </listener-class>  </listener>  <filter>  <filter-name>springSecurityFilterChain</filter-name> <filter-class>org.springframework.web.filter.DelegatingFilterProxy</filter-class>  </filter>  <filter-mapping>  <filter-name>springSecurityFilterChain</filter-name>  <url-pattern>/\*</url-pattern>  </filter-mapping> |

（2）manager的spring目录下添加配置文件spring-security.xml

|  |
| --- |
| <?xml version=*"1.0"* encoding=*"UTF-8"*?>  <beans:beans xmlns=*"http://www.springframework.org/schema/security"*  xmlns:beans=*"http://www.springframework.org/schema/beans"* xmlns:xsi=*"http://www.w3.org/2001/XMLSchema-instance"*  xsi:schemaLocation=*"http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-beans.xsd*  *http://www.springframework.org/schema/security http://www.springframework.org/schema/security/spring-security.xsd"*>  <!-- 以下页面不被拦截 -->  <http pattern=*"/login.html"* security=*"none"*></http>  <http pattern=*"/css/\*\*"* security=*"none"*></http>  <http pattern=*"/img/\*\*"* security=*"none"*></http>  <http pattern=*"/js/\*\*"* security=*"none"*></http>  <http pattern=*"/plugins/\*\*"* security=*"none"*></http>    <!-- 页面拦截规则 -->  <!-- use-expressions:设置是否启动SpEL表达式，默认值是true。 -->  <http use-expressions=*"false"*>  <!--  配置SpringSecurity的拦截路径（拦截规则）  \* pattern:配置拦截规则。 /\* 代表的是根路径下的所有资源（不包含子路径） /\*\*代表的是根路径下所有的资源（包含子路径）  \* access:设置角色 角色命名 ROLE\_角色名称 如： ROLE\_USER  -->  <intercept-url pattern=*"/\*\*"* access=*"ROLE\_ADMIN"* />  <!--  开启表单验证  username-parameter="username"  password-parameter="password"  login-page :登录页面名称 以 / 开始  default-target-url :登录成功后跳转的页面  login-processing-url:提交的路径的设置 默认值"/login" 可以修改  -->  <form-login login-page=*"/login.html"* default-target-url=*"/admin/index.html"* authentication-failure-url=*"/login.html"* always-use-default-target=*"true"*/>  <!-- 不使用csrf的校验 -->  <csrf disabled=*"true"*/>  <headers>  <!-- 配置框架页面不拦截 -->  <frame-options policy=*"SAMEORIGIN"*/>  </headers>  </http>  <!-- 认证管理器 -->  <authentication-manager>  <authentication-provider>  <user-service>  <user name=*"admin"* password=*"123456"* authorities=*"ROLE\_ADMIN"*/>  <user name=*"sunwukong"* password=*"dasheng"* authorities=*"ROLE\_ADMIN"*/>  </user-service>  </authentication-provider>  </authentication-manager>  </beans:beans> |

配置说明：

always-use-default-target：指定了是否在身份验证通过后总是跳转到default-target-url属性指定的URL。

如果你在系统中使用了框架页，那么在spring-security.xml中需要设置框架页的策略为SAMEORIGIN

|  |
| --- |
| <headers>  <frame-options policy=*"SAMEORIGIN"*/>  </headers> |

### 2.2.2登录页面

修改pinyougou-web-manager的 login.html

|  |
| --- |
| <form id=*"loginform"* action=*"/login"* method=*"post"* class=*"sui-form"*>  <div class=*"input-prepend"*><span class=*"add-on loginname"*></span>  <input id=*"prependedInput"* name=*"username"* type=*"text"* placeholder=*"邮箱/用户名/手机号"* class=*"span2 input-xfat"*>  </div>  <div class=*"input-prepend"*><span class=*"add-on loginpwd"*></span>  <input id=*"prependedInput"* name=*"password"* type=*"password"* placeholder=*"请输入密码"* class=*"span2 input-xfat"*>  </div>  <div class=*"setting"*>  <div id=*"slider"*>  <div id=*"slider\_bg"*></div>  <span id=*"label"*>>></span> <span id=*"labelTip"*>拖动滑块验证</span>  </div>  </div>  <div class=*"logined"*>  <a class=*"sui-btn btn-block btn-xlarge btn-danger"* onclick="document:loginform.submit()" target=*"\_blank"*>登&nbsp;&nbsp;录</a>  </div>  </form> |

## 2.3主界面显示登陆人

### 2.3.1后端代码

在pinyougou-manager-web新建LoginController.java

|  |
| --- |
| **package** com.pinyougou.manager.controller;  **import** java.util.HashMap;  **import** java.util.Map;  **import** org.springframework.security.core.context.SecurityContextHolder;  **import** org.springframework.security.core.userdetails.UserDetails;  **import** org.springframework.web.bind.annotation.RequestMapping;  **import** org.springframework.web.bind.annotation.RestController;  @RestController  @RequestMapping("/login")  **public** **class** LoginController {  @RequestMapping("/showName")  **public** Map name(){  String name=SecurityContextHolder.*getContext*()  .getAuthentication().getName();  Map map=**new** HashMap();  map.put("userName", name);  **return** map ;  }  } |

### 2.3.2前端代码

1. 新建loginService.js

|  |
| --- |
| //登陆服务层  app.service('loginService',**function**($http){  //读取登录人名称  **this**.loginName=**function**(){  **return** $http.get('../login/showName.do');  }  }); |

1. 新建indexController.js

|  |
| --- |
| app.controller('indexController' ,**function**($scope,$controller ,loginService){  //读取当前登录人  $scope.showLoginName=**function**(){  loginService.loginName().success(  **function**(response){  $scope.loginName=response.username;  }  );  }  }); |

index.html页面上引入JS

|  |
| --- |
| <script type=*"text/javascript"* src=*"../plugins/angularjs/angular.min.js"*></script>  <script type=*"text/javascript"* src=*"../js/base.js"*></script>  <script type=*"text/javascript"* src=*"../js/service/loginService.js"*></script>  <script type=*"text/javascript"* src=*"../js/controller/indexController.js"*></script> |

指令

|  |
| --- |
| <body class=*"hold-transition skin-green sidebar-mini"* ng-app=*"pinyougou"* ng-controller=*"indexController" ng-init="*showLoginName*()">* |

将页面上的测试用户 替换成 {{loginName}}

## 2.4退出登录

在pinyougou-web-manager的spring-security.xml的http节点中添加配置

|  |
| --- |
| <logout logout-url=*"/logout"* logout-success-url=*"/login.html"*/> |

加此配置后，会自动的产生退出登录的地址/logout,如果你不想用这个地址 ，你也可以定义生成的退出地址以及跳转的页面，配置如下

logout-url:退出的地址，会自动生成

logout-success-url:退出后跳转的地址

修改注销的链接

|  |
| --- |
| <div class=*"pull-right"*>  <a href=*"../logout"* class=*"btn btn-default btn-flat"*>注销</a>  </div> |

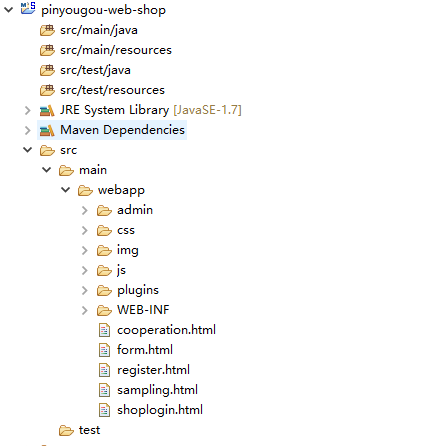
# 3.商家申请入驻

## 3.1需求分析

商家申请入驻，需要填写商家相关的信息。待运营商平台审核通过后即可使用使用。

## 3.2准备工作

（1）拷贝资源： 将“资源/ 01成品页面/ shop-web”下的页面拷贝到pinyougou-shop-web工程



1. 拷贝资源: 将“资源/ 03配置文件/第一天搭建/ shop-web”下的配置文件拷贝到shop工程

## 3.3前端代码

修改register.html 引入JS

|  |
| --- |
| <script type=*"text/javascript"* src=*"plugins/angularjs/angular.min.js"*> </script>  <script type=*"text/javascript"* src=*"js/base.js"*> </script>  <script type=*"text/javascript"* src=*"js/service/sellerService.js"*> </script>  <script type=*"text/javascript"* src=*"js/controller/baseController.js"*> </script>  <script type=*"text/javascript"* src=*"js/controller/sellerController.js"*> </script> |

指令

|  |
| --- |
| <body ng-app=*"pinyougou"* ng-controller=*"sellerController"*> |

绑定表单（部分代码）

|  |
| --- |
| <div class=*"control-group"*>  <label class=*"control-label"*>登陆名（不可修改）：</label>  <div class=*"controls"*>  <input type=*"text"* ng-model=*"entity.sellerId"* placeholder=*"登陆名"* class=*"input-xfat input-xlarge"*>  </div>  </div>  <div class=*"control-group"*>  <label class=*"control-label"*>登陆密码：</label>  <div class=*"controls"*>  <input type=*"password"* ng-model=*"entity.password"* placeholder=*"登陆密码"* class=*"input-xfat input-xlarge"*>  </div>  </div>  <div class=*"control-group"*>  <label class=*"control-label"*>店铺名称：</label>  <div class=*"controls"*>  <input ng-model=*"entity.nickName"* type=*"text"* placeholder=*"店铺名称"* class=*"input-xfat input-xlarge"*>  </div>  </div>  <div class=*"control-group"*>  <label class=*"control-label"*>公司名称：</label>  <div class=*"controls"*>  <input ng-model=*"entity.name"* type=*"text"* placeholder=*"公司名称"* class=*"input-xfat input-xlarge"*>  </div>  </div>  <div class=*"control-group"*>  <label class=*"control-label"*>公司电话：</label>  <div class=*"controls"*>  <input ng-model=*"entity.telephone"* type=*"text"* placeholder=*"公司电话"* class=*"input-xfat input-xlarge"*>  </div>  </div>  <div class=*"control-group"*>  <label class=*"control-label"*>公司详细地址：</label>  <div class=*"controls"*>  <input ng-model=*"entity.addressDetail"* type=*"text"* placeholder=*"公司详细地址"* class=*"input-xfat input-xlarge"*>  </div>  </div>  ..............略 |

修改sellerController.js ，在保存成功后跳转到登陆页

|  |
| --- |
| //保存  $scope.add=**function**(){  sellerService.add( $scope.entity ).success(  **function**(response){  **if**(response.success){  location.href='shoplogin.html';  }**else**{  alert(response.message);  }  }  );  } |

绑定register.html 页面“申请入驻”按钮

|  |
| --- |
| <a class=*"sui-btn btn-block btn-xlarge btn-danger"* ng-click=*"add()"* target=*"\_blank"*>申请入驻</a> |

## 3.4后端代码

pinyougou-interface项目中加入

|  |
| --- |
| **public** **interface** SellerService {    **public** **void** add(Seller seller);    } |

编写后端代码pinyougou-service-sellergoods的SellerServiceImpl类的add方法，设置默认状态为0

|  |
| --- |
| /\*\*  \* 商家管理  \* **@author** lx  \*  \*/  @Service  @Transactional  **public** **class** SellerServiceImpl **implements** SellerService {  @Autowired  **private** SellerDao sellerDao;  //添加商品  **public** **void** add(Seller seller){  //未审核的商品  seller.setStatus("0");  //商品 注册 的时间  seller.setCreateTime(**new** Date());  sellerDao.insertSelective(seller);    }  } |

Pinyougou-shop-web项目中加入

|  |
| --- |
| @RestController  @RequestMapping("/seller")  **public** **class** SellerController {    @Reference  **private** SellerService sellerService;    @RequestMapping("/add")  **public** Result add(@RequestBody Seller seller) **throws** Exception {  **try** {  sellerService.add(seller);  **return** **new** Result(**true**, "添加成功!");  } **catch** (Exception e) {  e.printStackTrace();  **return** **new** Result(**false**, "添加失败!");  }  }    } |

# 4.商家审核(同学们完成)

## 4.1需求分析

商家申请入驻后，需要网站运营人员在运营商后台进行审核，审核后商家才可以登陆系统。

**状态值：** 0：未审核 1：已审核 2：审核未通过 3：关闭

## 4.2商家待审核列表

修改manager-web系统seller\_1.html

引入JS

|  |
| --- |
| <script type=*"text/javascript"* src=*"../plugins/angularjs/angular.min.js"*> </script>  <!-- 分页组件开始 -->  <script src=*"../plugins/angularjs/pagination.js"*></script>  <link rel=*"stylesheet"* href=*"../plugins/angularjs/pagination.css"*>  <!-- 分页组件结束 -->  <script type=*"text/javascript"* src=*"../js/base\_pagination.js"*> </script>  <script type=*"text/javascript"* src=*"../js/service/sellerService.js"*> </script>  <script type=*"text/javascript"* src=*"../js/controller/baseController.js"*> </script>  <script type=*"text/javascript"* src=*"../js/controller/sellerController.js"*> </script> |

指令

|  |
| --- |
| <body class=*"hold-transition skin-red sidebar-mini"* ng-app=*"pinyougou"* ng-controller=*"sellerController"* ng-init="searchEntity={status:'0'}*"*> |

加入分页控件

|  |
| --- |
| <tm-pagination conf=*"paginationConf"*></tm-pagination> |

循环

|  |
| --- |
| <tr ng-repeat=*"entity in list"*>  <td><input type=*"checkbox"*></td>  <td>{{entity.sellerId}}</td>  <td>{{entity.name}}</td>  <td>{{entity.nickName}}</td>  <td>{{entity.linkmanName}}</td>  <td>{{entity.telephone}}</td>  <td class=*"text-center"*>  <button type=*"button"* class=*"btn bg-olive btn-xs"* data-toggle=*"modal"* data-target=*"#sellerModal"* >详情</button>  </td>  </tr> |

## 4.3商家详情



（1）绑定页面弹出窗口

|  |
| --- |
| <table class=*"table table-bordered table-striped"* width=*"800px"*>  <tr>  <td>公司名称</td>  <td>{{entity.name}}</td>  </tr>  <tr>  <td>公司手机</td>  <td>{{entity.mobile}}</td>  </tr>  <tr>  <td>公司电话</td>  <td>{{entity.telephone}}</td>  </tr>  <tr>  <td>公司详细地址</td>  <td>{{entity.addressDetail}}</td>  </tr>  </table> |

（2）列表的“详情”按钮

|  |
| --- |
| <button type=*"button"* class=*"btn bg-olive btn-xs"* data-toggle=*"modal"* data-target=*"#sellerModal"* ng-click=*"findOne(entity.sellerId)"*>详情</button> |

## 4.4商家审核

### 4.4.1 后端代码

在pinyougou-sellergoods-service的SellerServiceImpl.java新增方法

|  |
| --- |
| @Autowired  **private** SellerDao sellerDao;      //搜索  **public** PageResult search(Seller seller,Integer pageNum,Integer pageSize){  PageHelper.*startPage*(pageNum, pageSize);  SellerQuery sellerQuery = **new** SellerQuery();  //查询未审核状态  sellerQuery.createCriteria().andStatusEqualTo(seller.getStatus());  Page<Seller> page = (Page<Seller>) sellerDao.selectByExample(sellerQuery);  **return** **new** PageResult(page.getTotal(), page.getResult());  }    //添加商品  **public** **void** add(Seller seller){    BCryptPasswordEncoder encoder = **new** BCryptPasswordEncoder();  //未审核的商品  seller.setStatus("0");  //商品 注册 的时间  seller.setCreateTime(**new** Date());  //对密码进行加密  seller.setPassword(encoder.encode(seller.getPassword()));  sellerDao.insertSelective(seller);    }  //通过ID查询一个商品  **public** Seller findOne(String sellerId){  **return** sellerDao.selectByPrimaryKey(sellerId);  }    //审核  **public** **void** updateStatus(String sellerId,String status){  Seller seller = **new** Seller();  seller.setSellerId(sellerId);  seller.setStatus(status);  sellerDao.updateByPrimaryKeySelective(seller);  } |

在pinyougou-web-manager的SellerController.java新增方法

|  |
| --- |
| /\*\*  \* 商家管理  \* **@author** lx  \*  \*/  @RestController  **public** **class** SellerController {    @Reference  **private** SellerService sellerService;    //添加商家  @RequestMapping(value = "/seller/add.do")  **public** Result add(@RequestBody Seller seller){  **try** {  sellerService.add(seller);  **return** **new** Result(**true**,"注册成功");  } **catch** (Exception e) {  // **TODO**: handle exception  **return** **new** Result(**false**,"注册失败");  }  }  //搜索  @RequestMapping(value = "/seller/search.do")  **public** PageResult search(@RequestBody Seller seller,Integer page,Integer rows){    **return** sellerService.search(seller, page, rows);    }  //通过商家名称（ID　）　　查询一个商品信息  @RequestMapping(value = "/seller/findOne.do")  **public** Seller findOne(String id){  **return** sellerService.findOne(id);  }  //审核  @RequestMapping(value = "/seller/updateStatus.do")  **public** Result updateStatus(String sellerId,String status){  **try** {  sellerService.updateStatus(sellerId, status);  **return** **new** Result(**true**,"审核成功");  } **catch** (Exception e) {  // **TODO**: handle exception  **return** **new** Result(**false**,"审核失败");  }    }} |

### 4.4.2 前端代码

修改manager的sellerService.js

|  |
| --- |
| //更改状态  **this**.updateStatus=**function**(sellerId,status){  **return** $http.get('../seller/updateStatus.do?sellerId='+sellerId+'&status='+status);  } |

修改pinyougou-manager-web的sellerController.js

|  |
| --- |
| $scope.updateStatus=**function**(sellerId,status){  sellerService.updateStatus(sellerId,status).success(  **function**(response){  **if**(response.flag){  $scope.reloadList();//刷新列表  }**else**{  alert(response.message);  }  }  );  } |

修改按钮，调用方法

|  |
| --- |
| <div class=*"modal-footer"*>  <button class=*"btn btn-success"* data-dismiss=*"modal"* aria-hidden=*"true"* ng-click=*"updateStatus(entity.sellerId,'1')"*>审核通过</button>  <button class=*"btn btn-danger"* data-dismiss=*"modal"* aria-hidden=*"true"* ng-click=*"updateStatus(entity.sellerId,'2')"*>审核未通过</button>  <button class=*"btn btn-danger"* data-dismiss=*"modal"* aria-hidden=*"true"* ng-click=*"updateStatus(entity.sellerId,'3')"*>关闭商家</button>  <button class=*"btn btn-default"* data-dismiss=*"modal"* aria-hidden=*"true"*>关闭</button>  </div> |

# 5.商家系统登录与安全控制

## 5.1需求分析

完成商家系统登陆与安全控制，商家账号来自数据库，并实现密码加密

在we-shop系统的web.xml中加入

|  |
| --- |
| <!-- 权限 -->  <context-param>  <param-name>contextConfigLocation</param-name>  <param-value>classpath:spring/spring-security.xml</param-value>  </context-param>  <listener>  <listener-class>  org.springframework.web.context.ContextLoaderListener  </listener-class>  </listener>  <filter>  <filter-name>springSecurityFilterChain</filter-name>  <filter-class>org.springframework.web.filter.DelegatingFilterProxy</filter-class>  </filter>  <filter-mapping>  <filter-name>springSecurityFilterChain</filter-name>  <url-pattern>/\*</url-pattern>  </filter-mapping> |

shoplogin.html.页面

|  |
| --- |
| <form id=*"loginform"* action=*"/login"* method=*"post"* class=*"sui-form"*>  <div class=*"input-prepend"*><span class=*"add-on loginname"*></span>  <input name=*"username"* id=*"prependedInput"* type=*"text"* placeholder=*"邮箱/用户名/手机号"* class=*"span2 input-xfat"*>  </div>  <div class=*"input-prepend"*><span class=*"add-on loginpwd"*></span>  <input name=*"password"* id=*"prependedInput"* type=*"password"* placeholder=*"请输入密码"* class=*"span2 input-xfat"*>  </div>  <div class=*"setting"*>  <label class=*"checkbox inline"*><input name=*"m1"* type=*"checkbox"* value=*"2"* checked=*""*>自动登录</label>  <span class=*"forget"*>忘记密码？</span>  </div>  <div class=*"logined"*>  <a class=*"sui-btn btn-block btn-xlarge btn-danger"* onclick="document:loginform.submit()" target=*"\_blank"*>登&nbsp;&nbsp;录</a>  </div>  </form> |

## 5.2自定义认证类

1. 在pinyougou-shop-web创建com.pinyougou.service包，包下创建类UserDetailsServiceImpl.java 实现UserDetailsService接口

|  |
| --- |
| **package** com.pinyougou.service;  **import** java.util.ArrayList;  **import** java.util.List;  **import** org.springframework.security.core.GrantedAuthority;  **import** org.springframework.security.core.authority.SimpleGrantedAuthority;  **import** org.springframework.security.core.userdetails.User;  **import** org.springframework.security.core.userdetails.UserDetails;  **import** org.springframework.security.core.userdetails.UserDetailsService;  /\*\*  \* 认证类  \* **@author** Administrator  \*  \*/  **public** **class** UserDetailsServiceImpl **implements** UserDetailsService {  @Override  **public** UserDetails loadUserByUsername(String username) **throws** Exception {  List<GrantedAuthority> grantedAuths = **new** ArrayList<GrantedAuthority>();  grantedAuths.add(**new** SimpleGrantedAuthority("ROLE\_SELLER"));  **return** **new** User(username,"123456", grantedAuths);  }  } |

1. 在pinyougou-shop-web的spring目录下创建spring-security.xml

|  |
| --- |
| <?xml version=*"1.0"* encoding=*"UTF-8"*?>  <beans:beans xmlns=*"http://www.springframework.org/schema/security"*  xmlns:beans=*"http://www.springframework.org/schema/beans"* xmlns:dubbo=*"http://code.alibabatech.com/schema/dubbo"* xmlns:xsi=*"http://www.w3.org/2001/XMLSchema-instance"*  xsi:schemaLocation=*"http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-beans.xsd*  *http://code.alibabatech.com/schema/dubbo http://code.alibabatech.com/schema/dubbo/dubbo.xsd*  *http://www.springframework.org/schema/security http://www.springframework.org/schema/security/spring-security.xsd"*>  <!-- 以下页面不被拦截 -->  <http pattern=*"/\*.html"* security=*"none"*></http>  <http pattern=*"/css/\*\*"* security=*"none"*></http>  <http pattern=*"/img/\*\*"* security=*"none"*></http>  <http pattern=*"/js/\*\*"* security=*"none"*></http>  <http pattern=*"/plugins/\*\*"* security=*"none"*></http>  <http pattern=*"/seller/add.do"* security=*"none"*></http>    <!-- 页面拦截规则 -->  <http use-expressions=*"false"*>  <intercept-url pattern=*"/\*\*"* access=*"ROLE\_SELLER"* />  <form-login login-page=*"/shoplogin.html"* default-target-url=*"/admin/index.html"* authentication-failure-url=*"/shoplogin.html"* always-use-default-target=*"true"*/>  <csrf disabled=*"true"*/>  <headers>  <frame-options policy=*"SAMEORIGIN"*/>  </headers>  </http>  <!-- 认证管理器 -->  <authentication-manager>  <authentication-provider user-service-ref=*"userDetailService"*>  </authentication-provider>  </authentication-manager>  <beans:bean id=*"userDetailService"* class=*"cn.itcast.core.service.UserDetailServiceImpl"*></beans:bean>  </beans:beans> |

经过上述配置，用户在输入密码123456时就会通过（用户名随意）

## 5.3认证类调用服务方法

修改UserDetailsServiceImpl.java ，添加属性和setter方法 ，修改loadUserByUsername方法

|  |
| --- |
| /\*\*  \* 认证类  \*  \* **@author** lx  \*  \*/  **public** **class** UserDetailServiceImpl **implements** UserDetailsService{  **private** SellerService sellerService;  **public** **void** setSellerService(SellerService sellerService) {  **this**.sellerService = sellerService;  }  @Override  **public** UserDetails loadUserByUsername(String username) **throws** UsernameNotFoundException {  // **TODO** Auto-generated method stub  Seller seller = sellerService.findOne(username);  **if**(**null** != seller){  **if**("1".equals(seller.getStatus())){  //审核通过的用户  List<GrantedAuthority> authorities = **new** ArrayList<GrantedAuthority>();  authorities.add(**new** SimpleGrantedAuthority("ROLE\_SELLER"));  **return** **new** User(seller.getSellerId(), seller.getPassword(), authorities);  }  }  //无此用户 返回NULL  **return** **null**;  } |

修改pinyougou-web-shop的spring-security.xml ，添加如下配置

|  |
| --- |
| <?xml version=*"1.0"* encoding=*"UTF-8"*?>  <beans:beans xmlns=*"http://www.springframework.org/schema/security"*  xmlns:beans=*"http://www.springframework.org/schema/beans"* xmlns:dubbo=*"http://code.alibabatech.com/schema/dubbo"* xmlns:xsi=*"http://www.w3.org/2001/XMLSchema-instance"*  xsi:schemaLocation=*"http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-beans.xsd*  *http://code.alibabatech.com/schema/dubbo http://code.alibabatech.com/schema/dubbo/dubbo.xsd*  *http://www.springframework.org/schema/security http://www.springframework.org/schema/security/spring-security.xsd"*>  <!-- 以下页面不被拦截 -->  <http pattern=*"/\*.html"* security=*"none"*></http>  <http pattern=*"/css/\*\*"* security=*"none"*></http>  <http pattern=*"/img/\*\*"* security=*"none"*></http>  <http pattern=*"/js/\*\*"* security=*"none"*></http>  <http pattern=*"/plugins/\*\*"* security=*"none"*></http>  <http pattern=*"/seller/add.do"* security=*"none"*></http>    <!-- 页面拦截规则 -->  <http use-expressions=*"false"*>  <intercept-url pattern=*"/\*\*"* access=*"ROLE\_SELLER"* />  <form-login login-page=*"/shoplogin.html"* default-target-url=*"/admin/index.html"* authentication-failure-url=*"/shoplogin.html"* always-use-default-target=*"true"*/>  <csrf disabled=*"true"*/>  <headers>  <frame-options policy=*"SAMEORIGIN"*/>  </headers>  </http>  <!-- 认证管理器 -->  <authentication-manager>  <authentication-provider user-service-ref=*"userDetailService"*>  </authentication-provider>  </authentication-manager>  <!-- 引用dubbo 服务 -->  <dubbo:application name=*"pinyougou-shop-web"* />  <dubbo:registry address=*"zookeeper://192.168.200.138:2181"*/>  <dubbo:reference id=*"sellerService"* interface=*"cn.itcast.core.service.SellerService"* >  </dubbo:reference>    <beans:bean id=*"userDetailService"* class=*"cn.itcast.core.service.UserDetailServiceImpl"*>  <beans:property name=*"sellerService"* ref=*"sellerService"*></beans:property>  </beans:bean>  </beans:beans> |

经过上述修改后，在登陆页输入用户名和密码与数据库一致即可登陆 。

## 5.4密码加密

### 5.4.1 BCrypt加密算法

用户表的密码通常使用MD5等不可逆算法加密后存储，为防止彩虹表破解更会先使用一个特定的字符串（如域名）加密，然后再使用一个随机的salt（盐值）加密。 特定字符串是程序代码中固定的，salt是每个密码单独随机，一般给用户表加一个字段单独存储，比较麻烦。 BCrypt算法将salt随机并混入最终加密后的密码，验证时也无需单独提供之前的salt，从而无需单独处理salt问题。

### 5.4.2商家入驻密码加密

商家申请入驻的密码要使用BCrypt算法进行加密存储，修改SellerController.java的add方法

|  |
| --- |
| /\*\*  \* 增加  \* **@param** seller  \* **@return**  \*/  @RequestMapping("/add")  **public** Result add(@RequestBody TbSeller seller){  //密码加密  BCryptPasswordEncoder passwordEncoder = **new** BCryptPasswordEncoder();  String password = passwordEncoder.encode(seller.getPassword());  seller.setPassword(password);  **try** {  sellerService.add(seller);  **return** **new** Result(**true**, "增加成功");  } **catch** (Exception e) {  e.printStackTrace();  **return** **new** Result(**false**, "增加失败");  }  } |

### 5.4.3加密配置

修改pinyougou-shop-web的spring-security.xml ，添加如下配置

|  |
| --- |
| <beans:bean id=*"bcryptEncoder"*  class=*"org.springframework.security.crypto.bcrypt.BCryptPasswordEncoder"* /> |

修改认证管理器的配置

|  |
| --- |
| <!-- 认证管理器 -->  <authentication-manager alias=*"authenticationManager"*>  <authentication-provider user-service-ref=*'userDetailService'*>  <password-encoder ref=*"bcryptEncoder"*></password-encoder>  </authentication-provider>  </authentication-manager> |

## 5.5显示登录名

参照运营商后台

## 5.6退出登录

参照运营商后台

Index.html

|  |
| --- |
| <div class=*"pull-right"*>  <a href=*"../logout"* class=*"btn btn-default btn-flat"*>注销</a>  </div> |

Spring-security.xml

|  |
| --- |
| <!-- 页面拦截规则 -->  <http use-expressions=*"false"*>  <intercept-url pattern=*"/\*\*"* access=*"ROLE\_SELLER"* />  <logout logout-url=*"/logout"* logout-success-url=*"/shoplogin.html"*/> |