# 什么是shiro

Apache Shiro是一个强大实用的java安全框架，可以提供给开发者直观并且综合的authentication（认证），authorization（授权），cryptography（加密）和session management（会话管理）

注：

1，shiro可以运行在任意环境，从最简单的命令行应用到最大的企业级web应用和（clustered）集群应用

2，Shiro不会去维护用户、维护权限，这些需要我们自己去设计/提供，然后通过相应的接口注入给Shiro

# RBAC

是基于角色的访问控制（Role-Based Access Control ）在 RBAC 中，权限与角色相关联，用户通过成为适当角色的成员而得到这些角色的权限。这就极大地简化了权限的管理。这样管理都是层级相互依赖的，权限赋予给角色，而把角色又赋予用户，这样的权限设计很清楚，管理起来很方便。

# Shiro基本组件描述

Application code

用户

SecurityManager

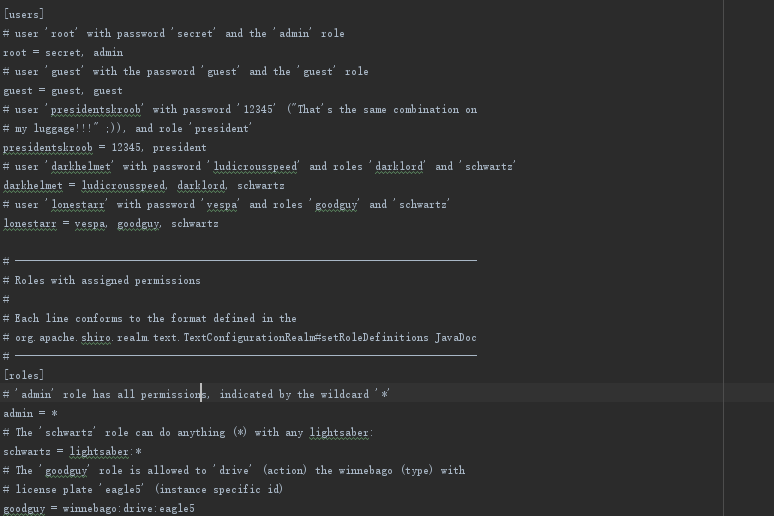
管理所有用户，核心

Realm

访问安全信息，进行验证

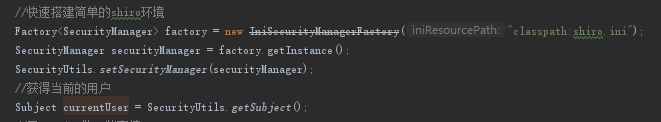
# 快速开始

## 首先写一个shiro的配置文件shiro.ini，文件中包括用户信息和权限，具体格式可查官方文档

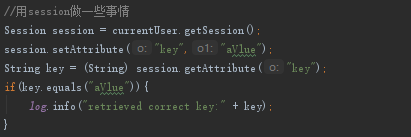


## 写一个测试类测试shiro

1，快速搭建shiro环境获得当前使用者



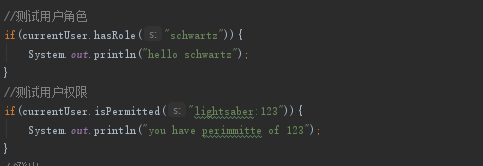
2，如果你想往当前用户对象中存入一些常用的东西，可以拿到用户的session并存入进去,但是session只对本次登陆有效



3，在未被验证前要进行登陆操作



4，根据登陆用户和权限进行操作



5，所有事情做完之后进行登出操作



# 关于认证（Authentication）

## 相关术语

1. subject：应用使用者，可以是人，第三方程序，服务连接等一切和你应用相关的东西
2. principals：身份：用户的识别属性，如用户名，安全号
3. credentials：证书，识别身份的秘密数据，如密码
4. realms：领域，用于安全信息的数据访问对象（DAO），应用组成部分，用于访问后台的安全信息数据源

## 怎么认证

1. 收集用户身份（principals）和证书（credentials）
2. 提交用户身份和证书到认证系统
3. 允许访问，重试认证或者阻止访问

注：步骤实现可看快速开始

# 关于授权（[Authorization](http://shiro.apache.org/java-authorization-guide.html" \l "elements-of-authorization)）

授权（也叫访问控制），规定了谁可以做什么

比如授权检查用户是否可以访问webapp，编辑数据。

## 授权的相关元素

1. Perssions：权限，是安全策略的原子级别，他们是功能声明。表示可以在程序中对什么资源做什么事情。和数据资源的相关的权限操作包括创建，读取，更新，删除，称为CRUD

需要注意的是权限权限不需要知道谁可以执行这些动作，他们仅仅声明了什么可以执行。

权限指定了对特定资源的特定操作

权限粒度：

资源级别（Resource Level）：这是最广泛的也是最容易建立的，资源被指定，但不是该资源的特定实例。比如用户可以编辑客户记录或打开门

实例级别（Instance Level）：权限指定资源的实例。比如用户可以编辑IBM的客户记录或打开厨房门。

属性级别（Attribute Level）：权限现在指定实例或资源的属性。比如用户可以编辑IBM客户记录上的地址。

1. Roles：角色，实际上是相关权限的集合，用来简化权限管理和用户管理，用户可以被分配角色而不是直接赋予权限

## 怎么执行授权检查

1. 通过编程方式，用if,else代码块执行授权检查
2. 通过注解，可以将注释添加到java代码中去
3. JSP/GSP标签库，可以基于角色和权限控制JSP或GSP页面输出

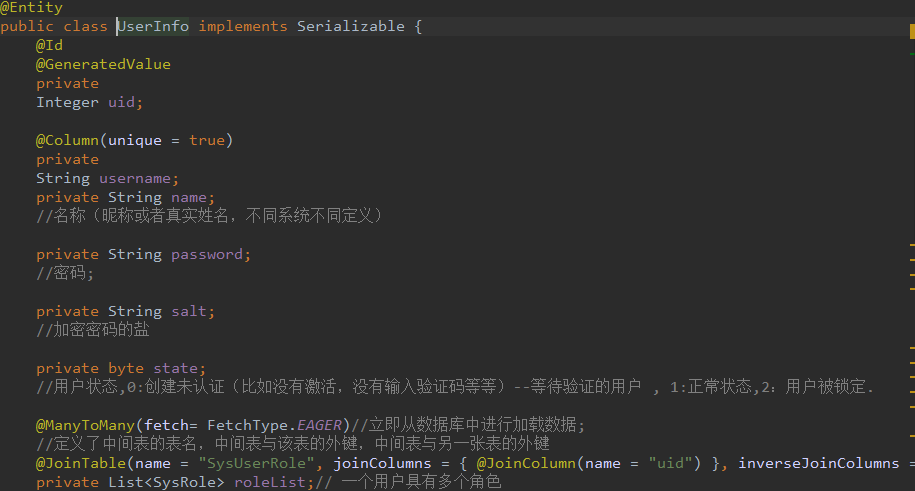
# Springboot结合shiro

## 引入相关依赖



## 采用jpa技术来自动生成基础表格

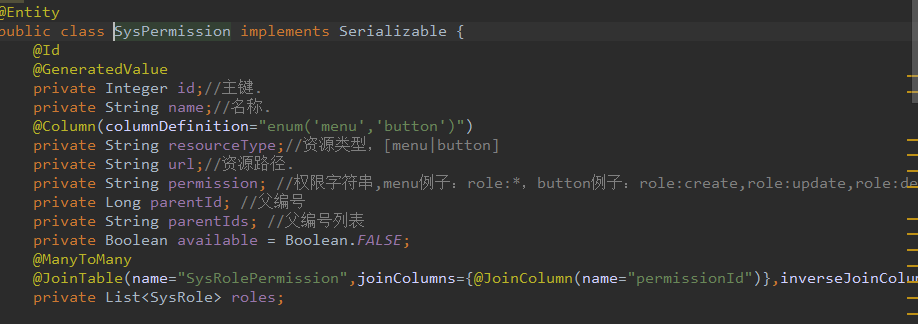
用户表



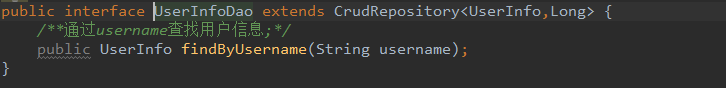
角色表



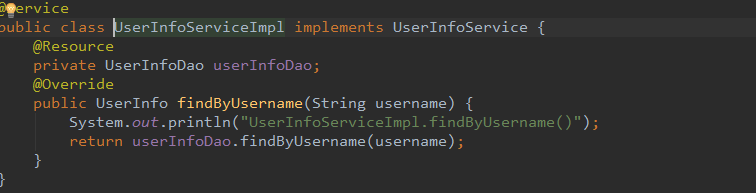
权限表



## 数据库查找dao

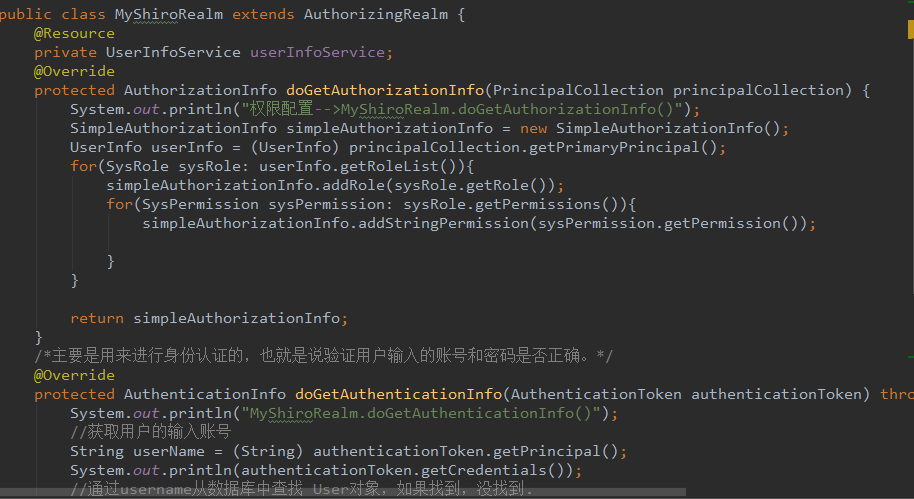


## service层



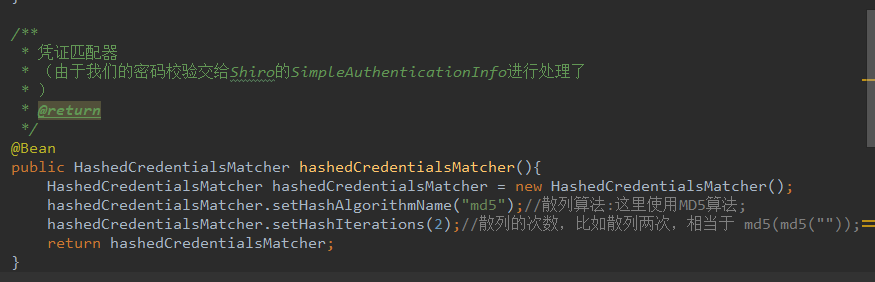
## 配置类

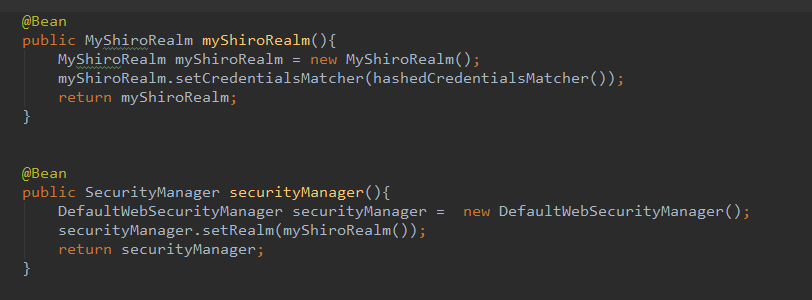
Ream配置

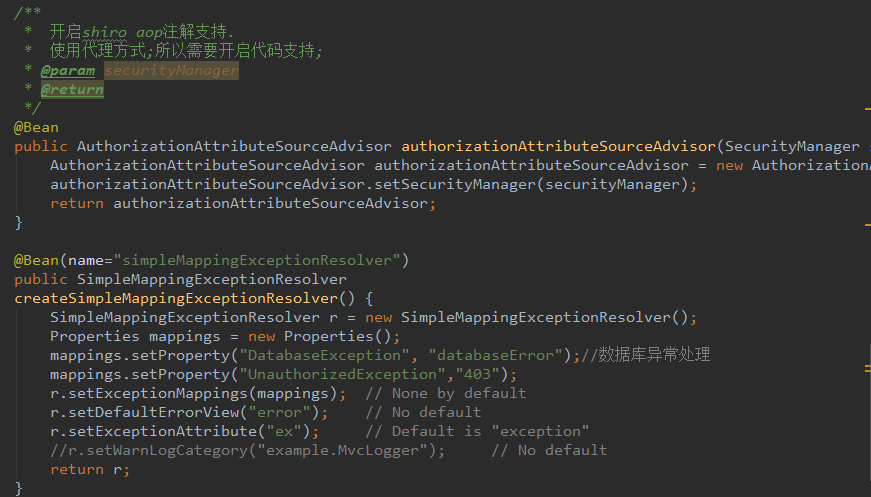


其将所有配置写入shiroConfig中

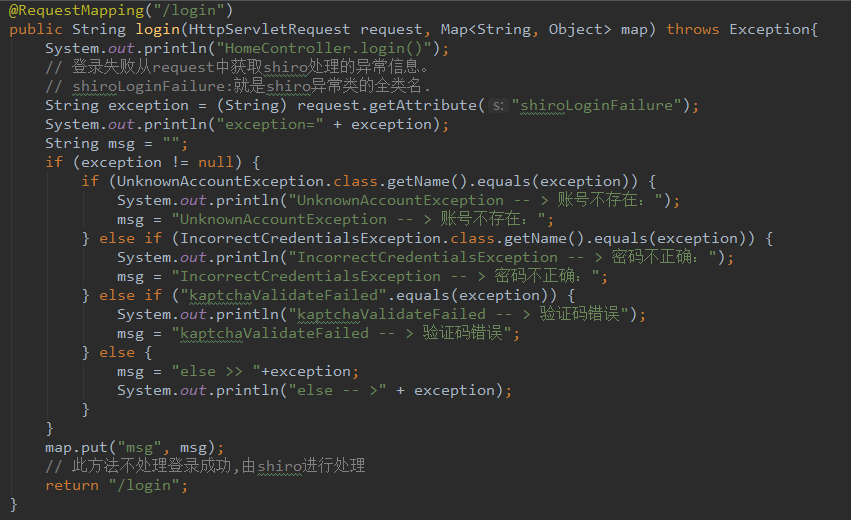




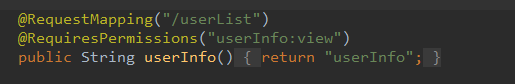




## 登陆controller



## 需要权限页面的controller



## 登陆页面

