# Day38\_Shiro安全管理框架

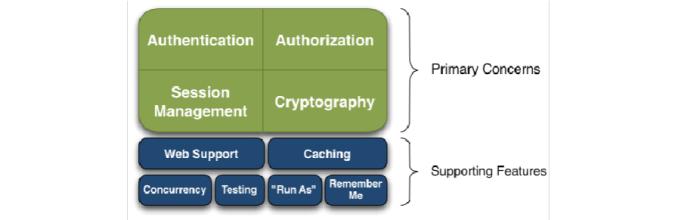
## Shiro简介

### 1.概念

Shiro是Apache提供的一套关于安全管理的框架.

Shiro框架主要可以用来实现认证,授权,加密,会话管理,缓存,

RememberMe,测试,RunAs,并发处理,与Web集成.



### 2.与Spring Security对比

Spring也提供了一个安全框架SpringSecurity,这个框架功能很全面也很强大,但是学习和入门的门槛比较高.Shiro相对来说就很轻量级,使用方便,但是对于实际开发中的绝大多数场景,Shiro都能够满足要求.

### 3.Shiro框架功能简介

①.Authentication:认证.主要是对用户的身份来进行认证,一般是在登陆的时候进行,验证用户是否拥有该身份.

②.Authorization:授权.主要是对用户的权限进行验证,以此来决定用户能够访问哪些页面资源.一方面可以从比较粗的粒度来验证用户的角色,另一方面可以从细的粒度来验证用户的权限.

③.SessionManager:会话管理.用户登录一次,就是一次会话.在用户退出之前,用户的信息都会保存在Session中.

④.Cryptography:加密功能.主要是将内容进行加密存储,比如把密码进行加密.

⑤.RememberMe:记住我.用户登录之后,下次再次访问,就不用登录了.

### 4.Shiro的核心API

①.Subject:主体.代表了当前操作的”用户”,该用户不一定是一个具体的人.每一个Subject都是与SecurityManager绑定在一起的,Subject与用户的所有交互,最终都是由SecurityManager来完成的,所以本质上,最核心的组件是SecurityManager.Subject类似于是一个”门面”.

②.SecurityManager:安全管理器.所有与安全相关的操作都是由SecurityManager来完成的,它管理着所有的Subject,是整个Shiro的核心.

③.Realm:域.Shiro框架本身不负责维护用户的身份/权限信息.所以此时就需要有一个Realm来负责程序员与Shiro的交互.所以Realm是程序员真正要关心的API.Shiro从Realm获取用户的权限/身份等信息,然后SecurityManager再验证用户信息.所以Realm可以被看成是一个”安全数据源”.

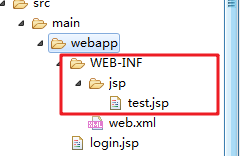
## SpringMVC补充知识点

如果我们要在浏览器中直接访问/WEB-INF/下的资源,默认是不允许的.

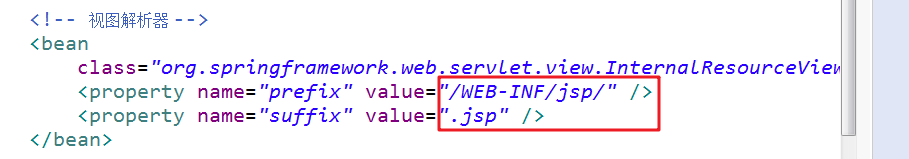
一般情况下,都需要创建一个Controller类,里面写一个跳转方法.

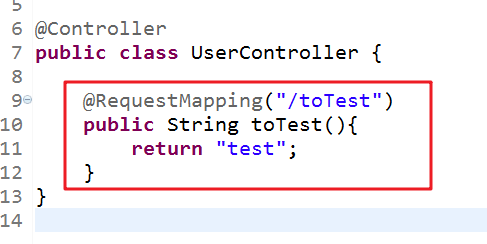
但是有时候我们不想那么麻烦,可以利用<mvc:view-controller>来快捷的实现该需求.

例如我们要访问如下资源:



#### 传统实现方案为:





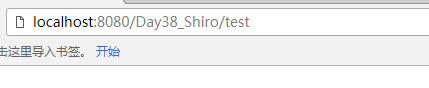
访问地址为:



#### 现在的解决方案:

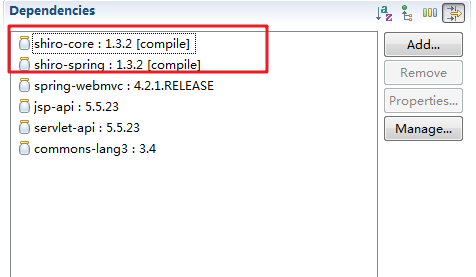


此时浏览器的访问地址为:

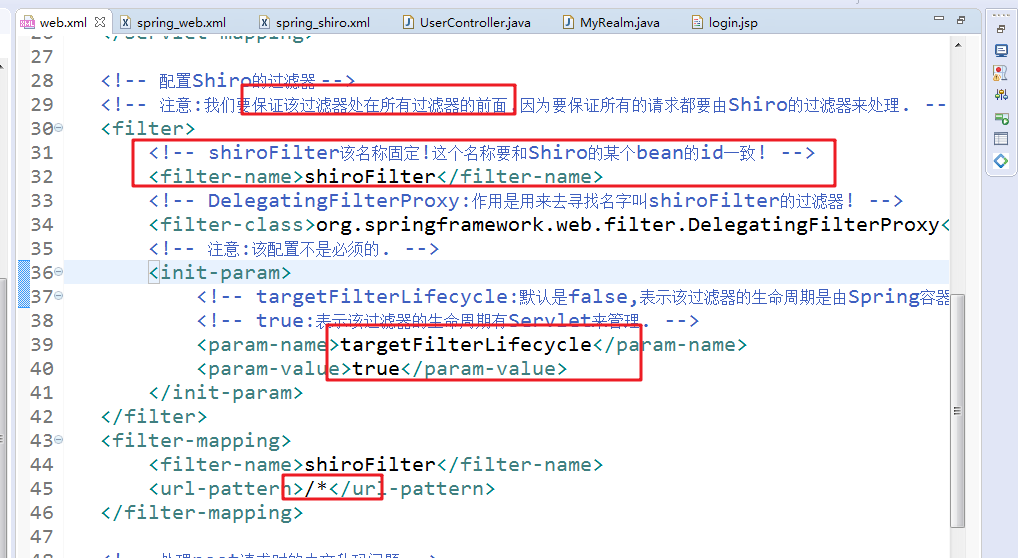


## Shiro开发实现

### 添加相关依赖包



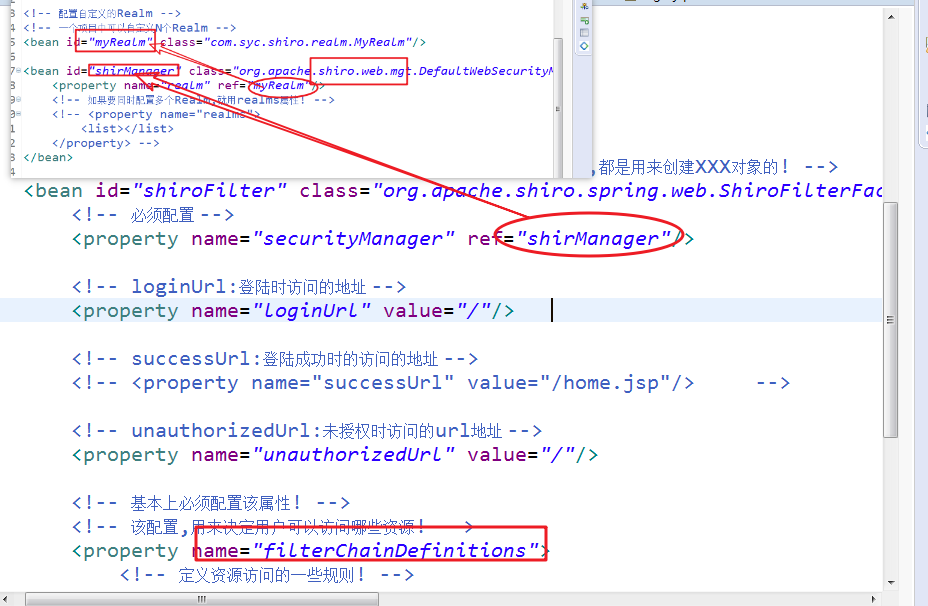
### 配置web.xml文件



### 3.配置spring\_web.xml文件

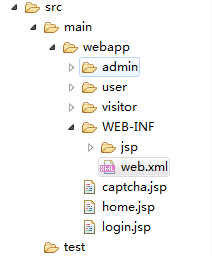


### 4.配置spring\_shiro.xml文件

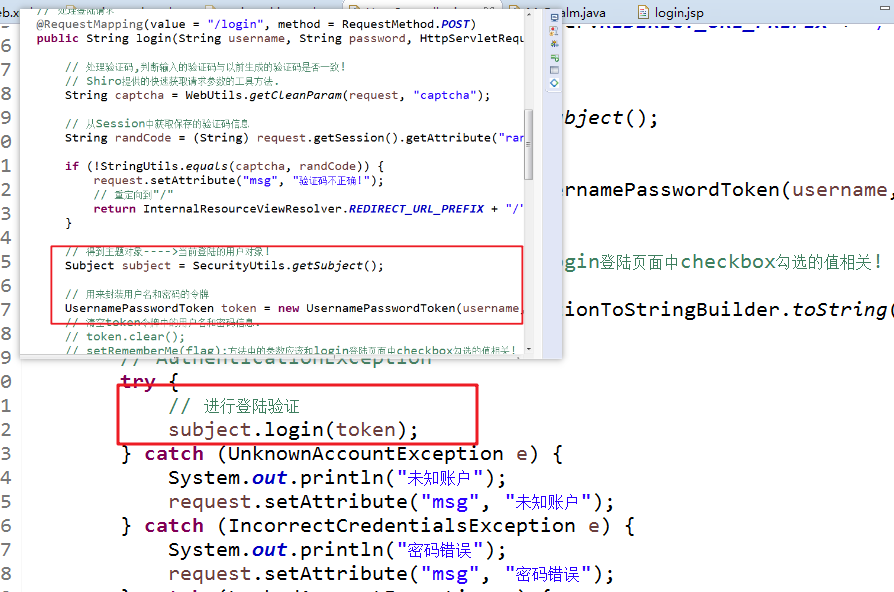




### 5.前端资源的创建



### 6.创建UserController控制器,处理用户请求

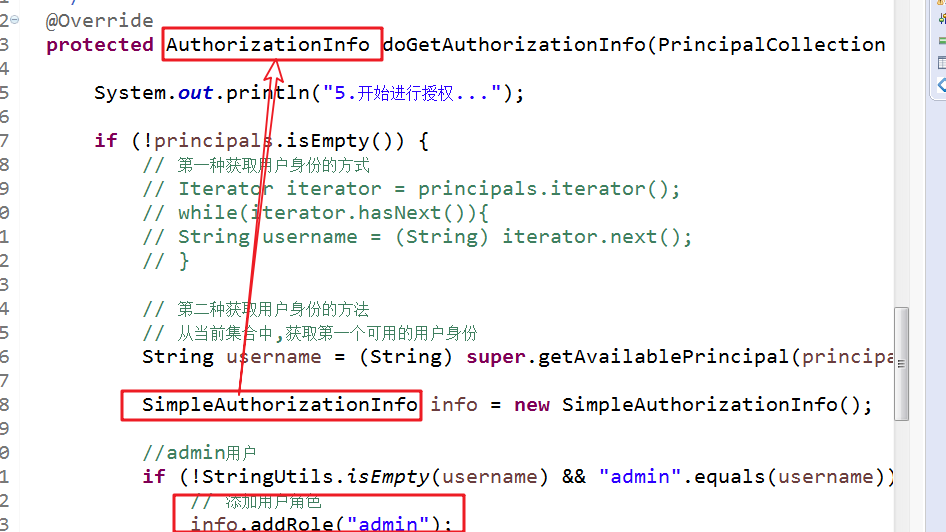


### 7.自定义Realm类,进行认证和授权的工作

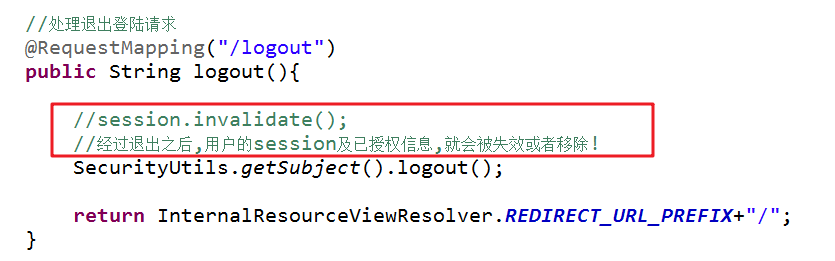
#### 实现认证方法:



#### 实现授权方法:



### 8.实现logout功能



## 细节分析

### Shiro的执行流程(从认证到授权....)

1. .在login.jsp页面中开始发起一个登陆请求,此时登陆页面输入了用户名和密码信息;
2. .进入到Controller类对应的请求方法中,利用Subject.login(token)方法开始认证的工作.
3. .自定义的Realm类doGetAuthenticationInfo(token)方法开始进行真正的认证操作,最终会返回一个SimpleAuthenticationInfo对象;
4. .进过第③步的认证,代码的执行重新返回到Controller类的请求方法中,准备进行下一步的操作.
5. .此时如果某些页面的访问需要经过授权才能访问,此时就会接着执行自定义的Realm类中的doGetAuthorizationInfo()方法,进行授权操作.

当授权完成后,用户就可以访问想要的资源了.

### UsernamePasswordToken中的password为什么用char[]类型,而不是String类型?

安全原因!

从String字符串本身的特点来进行分析.

加入String pwd=”123”;

String pwd=null;

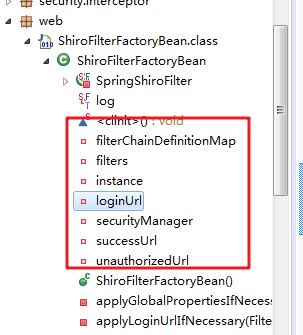
问:原先的密码内容123丢失了吗?---->仍然在内存中,所以不够安全!

如果char[] pwd=123;

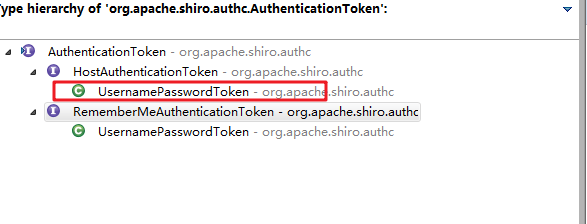
char[] pwd=0x00;

问:原先的密码内容123丢失了吗?---->原先的没了,0x00覆盖了原先的值!所以很安全....

### 3.ShiroFilterFactoryBean类的属性



### 4.AuthenticationToken的类关系图



### 5.Shiro的异常类结构图

