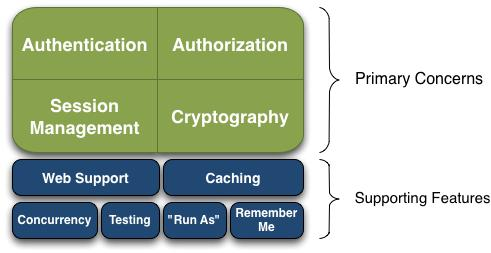
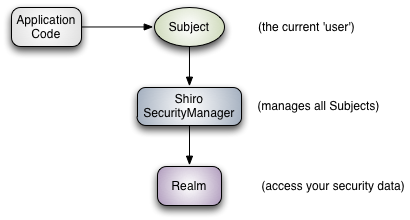
Shiro讲解

**一、什么是Shiro**   
Apache Shiro是一个强大易用的Java安全框架，提供了认证、授权、加密和会话管理等功能： 

* 认证 - 用户身份识别，常被称为用户“登录”；
* 授权 - 访问控制；
* 密码加密 - 保护或隐藏数据防止被偷窥；
* 会话管理 - 每用户相关的时间敏感的状态。
* 
* **Authentication：**身份认证/登录，验证用户是不是拥有相应的身份； **Authorization：**授权，即权限验证，验证某个已认证的用户是否拥有某个 权限；即判断用户是否能做事情，常见的如：验证某个用户是否拥有某个角 色。或者细粒度的验证某个用户对某个资源是否具有某个权限； **Session Manager：**会话管理，即用户登录后就是一次会话，在没有退出之前，它的所有信息都在会话中；会话可以是普通JavaSE环境的，也可以是如Web环境的
* **Cryptography：**加密，保护数据的安全性，如密码加密存储到数据库，而不是明文存储；
* **Web Support：**Web支持，可以非常容易的集成到Web环境；Caching：缓存，比如用户登录后，其用户信息、拥有的角色/权限不必每次去查，这样可以提高效率；
* **Concurrency：**shiro支持多线程应用的并发验证，即如在一个线程中开启另一个线程，能把权限自动传播过去；
* **Testing：**提供测试支持；
* **Run As：**允许一个用户假装为另一个用户（如果他们允许）的身份进行访问；
* **Remember Me：**记住我，这个是非常常见的功能，即一次登录后，下次再来的话不用登录了。

**二、Shiro的架构介绍**   
首先，来了解一下Shiro的三个核心组件：Subject, SecurityManager 和 Realms. 如下图：   
   
Subject：即“当前操作用户”。但是，在Shiro中，Subject这一概念并不仅仅指人，也可以是第三方进程、后台帐户（Daemon Account）或其他类似事物。它仅仅意味着“当前跟软件交互的东西”。但考虑到大多数目的和用途，你可以把它认为是Shiro的“用户”概念。   
Subject代表了当前用户的安全操作，SecurityManager则管理所有用户的安全操作。   
  
SecurityManager：它是Shiro框架的核心， Shiro通过SecurityManager来管理内部组件实例，并通过它来提供安全管理的各种服务。   
  
Realm： Realm充当了Shiro与应用安全数据间的“桥梁”或者“连接器”。也就是说，当对用户执行认证（登录）和授权（访问控制）验证时，Shiro会从应用配置的Realm中查找用户及其权限信息。

**Shiro内部架构图：**   
  
   
**Subject：**主体，可以看到主体可以是任何可以与应用交互的“用户”；

**SecurityManager ：**相当于SpringMVC 中的DispatcherServlet 或者Struts2 中的

FilterDispatcher；是Shiro的心脏；所有具体的交互都通过SecurityManager进行控制；它管

理着所有Subject、且负责进行认证和授权、及会话、缓存的管理。

**Authenticator：**认证器，负责主体认证的，这是一个扩展点，如果用户觉得Shiro 默认的

不好，可以自定义实现；其需要认证策略（Authentication Strategy），即什么情况下算用户

认证通过了；

**Authrizer：**授权器，或者访问控制器，用来决定主体是否有权限进行相应的操作；即控制

着用户能访问应用中的哪些功能；

**Realm：**可以有1个或多个Realm，可以认为是安全实体数据源，即用于获取安全实体的；

可以是JDBC 实现，也可以是LDAP 实现，或者内存实现等等；由用户提供；注意：Shiro

不知道你的用户/权限存储在哪及以何种格式存储；所以我们一般在应用中都需要实现自己

的Realm；

**SessionManager：**如果写过Servlet就应该知道Session的概念，Session呢需要有人去管理

它的生命周期，这个组件就是SessionManager；而Shiro 并不仅仅可以用在Web 环境，也

可以用在如普通的JavaSE 环境、EJB 等环境；所有呢，Shiro 就抽象了一个自己的Session

来管理主体与应用之间交互的数据；这样的话，比如我们在Web 环境用，刚开始是一台

Web 服务器；接着又上了台EJB 服务器；这时想把两台服务器的会话数据放到一个地方，

这个时候就可以实现自己的分布式会话（如把数据放到Memcached服务器）；

**SessionDAO：**DAO 大家都用过，数据访问对象，用于会话的CRUD，比如我们想把Session

保存到数据库，那么可以实现自己的SessionDAO，通过如JDBC 写到数据库；比如想把

Session 放到Memcached 中，可以实现自己的Memcached SessionDAO；另外SessionDAO

中可以使用Cache进行缓存，以提高性能；

**CacheManager：**缓存控制器，来管理如用户、角色、权限等的缓存的；因为这些数据基本

上很少去改变，放到缓存中后可以提高访问的性能

**Cryptography：**密码模块，Shiro 提高了一些常见的加密组件用于如密码加密/解密的。

**三、Shiro认证**

* 1. 以下就是实现了了一个完整的登录和登出操作



上面代码解释：

Subject subject = SecurityUtils.*getSubject*();

subject.login(token);

Subject收集用户实例后去提交认证，如果认证成功则subject.isAuthenticated()会返回为true,则表示用户认证通过，否则在subject.login是就抛出会异常，

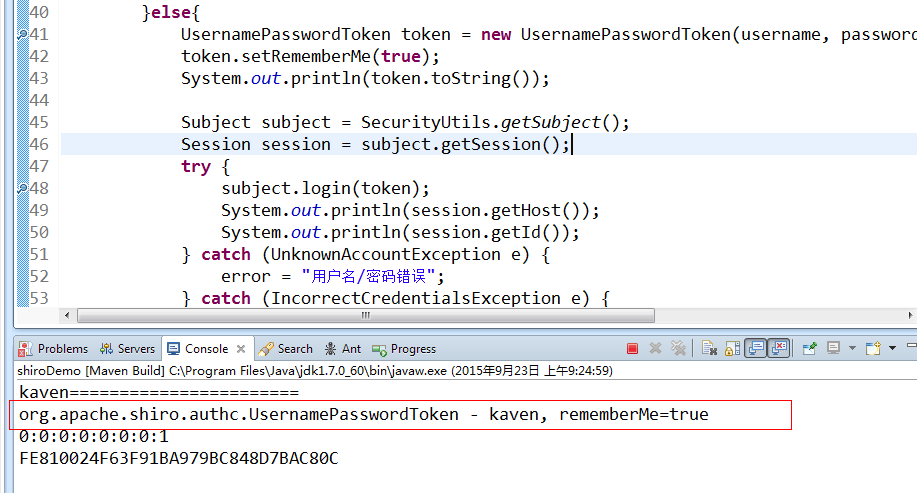
想退出是使用subject.lonout去执行登出操作

UsernamePasswordToken：

实现了用户名/密码的认证机制，同时它也实现了RememberMeAuthenticationToken接口，这个接口可以实现“记住我”的功能

以下运行结果表示身份验证通过：





以下是实现的Realm



subject.login(token);以后会把用户的token传入自己配置的Realm中 执行 doGetAuthenticationInfo方法进行身份验证

正常情况下Realm都是继承Reaml但是我们这里继承AuthorizingRealm类实现 doGetAuthorizationInfo() 验证是否授权方法 和doGetAuthenticationInfo()身份验证

**四、Realm的实现**

Realm的实现分俩种：

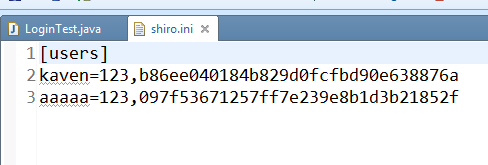
doGetAuthenticationInfo ()

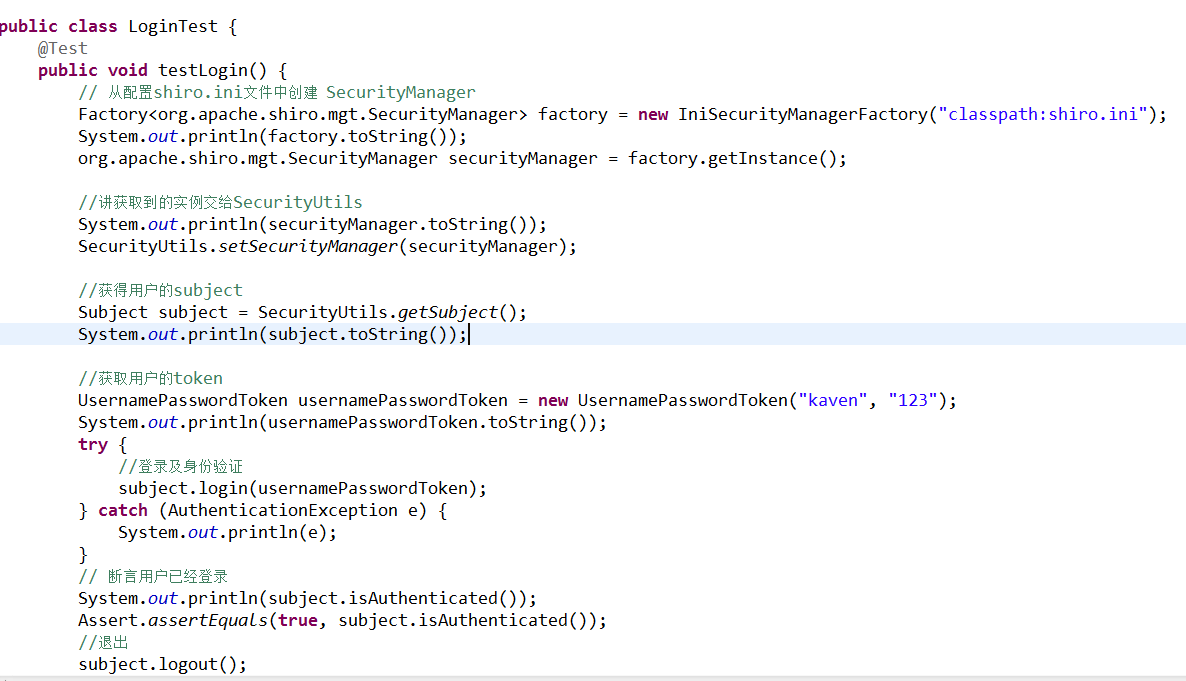
doGetAuthorizationInfo()

在shiro的认证过程最后都会交给Realm去实现,****

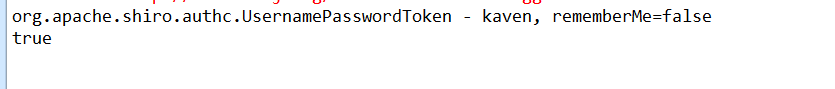
下面是一个基于读取配置文件实现的一个shiro版本：

采用myeclipse自带的juint运行,配置文件中的密码我们使用的是

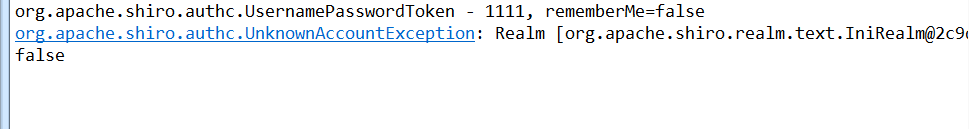




正常执行结果:



如果我们写入在没有配置文件的帐号 那么就会提示错误



以上是一个比较简单的 shiro认证 授权，

其他的:

session的管理

缓存的集成及使用

Shiro的拦截

Shiro的标签

数据的安全 加密

单点登录

SSL Oauth

还需要学习，在学习中shiro遇到的问题挺多，因为查找资料上面讲的很多配置他们是不会讲解，这个就需要花很多时间自己去寻找资料

Apache Shiro 简介

http://www.ibm.com/developerworks/cn/web/wa-apacheshiro/

在Web项目中应用Apache Shiro 开源权限框架

http://www.php100.com/html/itnews/it/2013/0206/12039.html

10分钟教会你Apache Shiro

http://www.cnblogs.com/ibook360/archive/2011/10/27/2226522.html

Apache Shiro 使用手册（一）Shiro架构介绍

http://kdboy.iteye.com/blog/1154644

Shiro+SroingMVC整合教程

http://blog.csdn.net/xkafei/article/details/21879209?utm\_source=tuicool

WhereTa角色权限管理系统

http://my.oschina.net/u/1792430/blog/505947

官网

http://shiro.apache.org/reference.html

myEclipse搭建Maven工程

http://blog.sina.com.cn/s/blog\_5543f1890102v1y8.html

Maven安装教程及Myeclipse搭建Maven工程

http://my.oschina.net/softwarechina/blog/134788

http://my.oschina.net/softwarechina/blog/134797

http://my.oschina.net/softwarechina/blog/219633

<http://jinnianshilongnian.iteye.com/blog/2018936>

重点资料：

https://github.com/zhangkaitao/shiro-example

http://jinnianshilongnian.iteye.com/blog/2018398