Springboot shiro 项目心得文档

# 创建项目

1. 创建数据库my\_world      表名分别为t\_base\_user，t\_base\_user\_role，t\_base\_role，t\_base\_menu\_role，t\_base\_menu
2. 通过mybatis plus自定义生成java代码（该工具完整版参考[https://github.com/admincjy/cjygenerator）](https://github.com/admincjy/cjygenerator%EF%BC%89" \t "_blank)
3. 创建springboot项目并引入相关jar包和代码（项目地址 [https://github.com/admincjy/shiro](http://xn--ces6a538pmb2a/)）
4. 注意：分页差距的依赖包需要引三个, 还需引入配置文件mybatis-config.xml(具体参考项目)                                                                             <!-- 分页依赖(引三个) -->  
   <dependency>  
   <groupId>com.github.pagehelper</groupId>  
   <artifactId>pagehelper</artifactId>  
   <version>5.0.1</version>  
   </dependency>  
   <dependency>  
   <groupId>com.github.pagehelper</groupId>  
   <artifactId>pagehelper-spring-boot-autoconfigure</artifactId>  
   <version>1.2.5</version>  
   </dependency>  
   <dependency>  
   <groupId>com.github.pagehelper</groupId>  
   <artifactId>pagehelper-spring-boot-starter</artifactId>  
   <version>1.2.5</version>  
   </dependency>

引入shiro的jar包  
<dependency>  
<groupId>org.apache.shiro</groupId>  
<artifactId>shiro-spring</artifactId>  
<version>1.4.0</version>  
</dependency>

<dependency>

<groupId>org.apache.shiro</groupId>

<artifactId>shiro-core</artifactId>

<version>1.4.0</version>

</dependency>

引入其他基本包

<dependency>  
<groupId>mysql</groupId>  
<artifactId>mysql-connector-java</artifactId>  
<scope>runtime</scope>  
</dependency>

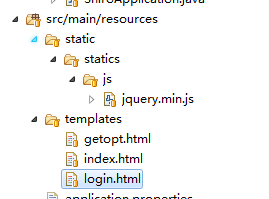
 <!-- mybatis两个包，不然用不了分页 -->  
<dependency>  
<groupId>com.baomidou</groupId>  
<artifactId>mybatis-plus-boot-starter</artifactId>  
<version>3.0.6</version>  
</dependency>  
<dependency>  
<groupId>com.alibaba</groupId>  
<artifactId>druid</artifactId>  
<version>1.1.8</version>  
</dependency>

<dependency>  
<groupId>org.springframework.boot</groupId>  
<artifactId>spring-boot-starter-web</artifactId>  
</dependency>

<dependency>  
<groupId>org.mybatis.spring.boot</groupId>  
<artifactId>mybatis-spring-boot-starter</artifactId>  
<version>1.3.2</version>  
</dependency>  
<dependency>  
<groupId>org.springframework.boot</groupId>  
<artifactId>spring-boot-starter-test</artifactId>  
<scope>test</scope>  
</dependency>

# 实现认证

**将静态html和js文件放入项目中，如图**：



**生成页面跳转类：（注意:页面跳转注解是@Controller不是@RestController）**

@Controller

@RequestMapping("/login")

public class LoginController {

@RequestMapping("/html")

public String loginHtml(){

return "/login";

}

@RequestMapping("/index")

public String indexHtml(){

return "/index";

}

@RequestMapping("/getopt")

public String getoptHtml(){

return "/getopt";

}

}

**自定义realm,这里我定义为MyShiroRealm:（注意:需配置config,不然数据库查询user无法查询要报异常）**

public class MyShiroRealm extends AuthorizingRealm{

@Autowired

private UserMapper userMapper;

/\*

\* 认证（非 Javadoc）

\* @see org.apache.shiro.realm.AuthorizingRealm#doGetAuthorizationInfo(org.apache.shiro.subject.PrincipalCollection)

\*/

@Override

protected AuthorizationInfo doGetAuthorizationInfo(PrincipalCollection principals) {

String username = (String)principals.getPrimaryPrincipal();

Set<String> roles = userMapper.findRoles(username);

Set<String> permissions = userMapper.findRoles(username);

SimpleAuthorizationInfo simpleAuthorizationInfo=new SimpleAuthorizationInfo();

simpleAuthorizationInfo.setRoles(roles);

simpleAuthorizationInfo.setStringPermissions(permissions);

return simpleAuthorizationInfo;

}

/\*

\* 认证（非 Javadoc）

\* @see org.apache.shiro.realm.AuthenticatingRealm#doGetAuthenticationInfo(org.apache.shiro.authc.AuthenticationToken)

\*/

@Override

protected AuthenticationInfo doGetAuthenticationInfo(AuthenticationToken token) throws AuthenticationException {

//从主体传过来的信息中获取用户的输入的账号.

UsernamePasswordToken tokens = (UsernamePasswordToken) token;

String username = tokens.getUsername();

//通过username从数据库中查找 User对象

//实际项目中，这里可以根据实际情况做缓存，如果不做，Shiro自己也是有时间间隔机制，2分钟内不会重复执行该方法

User user = this.findByUsername(username);

//创建返回对象

SimpleAuthenticationInfo authenticationInfo = new SimpleAuthenticationInfo(

username, //用户名

user.getPassword(), //密码

、、//ByteSource.Util.bytes(user.getUsername()+user.getSalt()),//salt=username+salt

getName() //realm name

);

return authenticationInfo;

}

public User findByUsername(String username){

User user = userMapper.findByUsername(username);

if(user == null){

return null;

}

return user;

}

}

**新建config类，我这取名为ShiroConfig：**

@Configuration

public class ShiroConfig {

/\*\*

\* 密码校验规则HashedCredentialsMatcher

\* 这个类是为了对密码进行编码的 ,

\* 防止密码在数据库里明码保存 , 当然在登陆认证的时候 ,

\* 这个类也负责对form里输入的密码进行编码

\* 处理认证匹配处理器：如果自定义需要实现继承HashedCredentialsMatcher

\*/

@Bean("hashedCredentialsMatcher")

public HashedCredentialsMatcher hashedCredentialsMatcher() {

HashedCredentialsMatcher credentialsMatcher = new HashedCredentialsMatcher();

//指定加密方式为MD5

credentialsMatcher.setHashAlgorithmName("MD5");

//加密次数

credentialsMatcher.setHashIterations(1);

credentialsMatcher.setStoredCredentialsHexEncoded(true);

return credentialsMatcher;

}

@Bean("authRealm")

@DependsOn("lifecycleBeanPostProcessor")//可选

public MyShiroRealm authRealm(@Qualifier("hashedCredentialsMatcher") HashedCredentialsMatcher matcher) {

MyShiroRealm authRealm = new MyShiroRealm();

authRealm.setAuthorizationCachingEnabled(false);

authRealm.setCredentialsMatcher(matcher);

return authRealm;

}

/\*\*

\* 定义安全管理器securityManager,注入自定义的realm

\* @param authRealm

\* @return

\*/

@Bean("securityManager")

public SecurityManager securityManager(@Qualifier("authRealm") MyShiroRealm authRealm) {

DefaultWebSecurityManager manager = new DefaultWebSecurityManager();

manager.setRealm(authRealm);

return manager;

}

/\*\*

\* 定义shiroFilter过滤器并注入securityManager

\* @param manager

\* @return

\*/

@Bean("shiroFilter")

public ShiroFilterFactoryBean shiroFilter(@Qualifier("securityManager") SecurityManager manager) {

ShiroFilterFactoryBean bean = new ShiroFilterFactoryBean();

//设置securityManager

bean.setSecurityManager(manager);

//设置登录页面

//可以写路由也可以写jsp页面的访问路径

bean.setLoginUrl("login/html");

//设置登录成功跳转的页面

bean.setSuccessUrl("/login/index");

//设置未授权跳转的页面

bean.setUnauthorizedUrl("/login/getopt");

//定义过滤器

LinkedHashMap<String, String> filterChainDefinitionMap = new LinkedHashMap<>();

filterChainDefinitionMap.put("/login/index", "authc");

filterChainDefinitionMap.put("/login/html", "anon");

filterChainDefinitionMap.put("/user/login", "anon");

// filterChainDefinitionMap.put("/admin", "roles[admin]");

// filterChainDefinitionMap.put("/edit", "perms[delete]");

// filterChainDefinitionMap.put("/druid/\*\*", "anon");

filterChainDefinitionMap.put("/statics/\*\*", "anon");

//需要登录访问的资源 , 一般将/\*\*放在最下边

filterChainDefinitionMap.put("/\*\*", "authc");

bean.setFilterChainDefinitionMap(filterChainDefinitionMap);

return bean;

}

/\*\*

\* Spring的一个bean , 由Advisor决定对哪些类的方法进行AOP代理 .

\* @return

\*/

@Bean

public DefaultAdvisorAutoProxyCreator defaultAdvisorAutoProxyCreator() {

DefaultAdvisorAutoProxyCreator creator = new DefaultAdvisorAutoProxyCreator();

creator.setProxyTargetClass(true);

return creator;

}

/\*\*

\* 配置shiro跟spring的关联

\* @param securityManager

\* @return

\*/

@Bean

public AuthorizationAttributeSourceAdvisor authorizationAttributeSourceAdvisor(@Qualifier("securityManager") SecurityManager securityManager) {

AuthorizationAttributeSourceAdvisor advisor = new AuthorizationAttributeSourceAdvisor();

advisor.setSecurityManager(securityManager);

return advisor;

}

/\*\*

\* lifecycleBeanPostProcessor是负责生命周期的 , 初始化和销毁的类

\* (可选)

\*/

@Bean("lifecycleBeanPostProcessor")

public LifecycleBeanPostProcessor lifecycleBeanPostProcessor() {

return new LifecycleBeanPostProcessor();

}

}

这里的注意事项：

SecurityManager 引包必须是import org.apache.shiro.mgt. SecurityManager;

credentialsMatcher.setHashIterations(1);只加密一次就设置为1，根据加密次数写

filterChainDefinitionMap.put("/statics/\*\*", "anon");静态js，css等文件放在Static下面新建的statics文件夹下，不要直接放在static下面，不然无法过滤

**在UserController里面创建注册和登陆的方法：**

/\*

\* 登陆

\*/

@RequestMapping("/login")

public BaseRespMsg login(String username,String password){

//把前端输入的username和password封装为token

UsernamePasswordToken token = new UsernamePasswordToken(username, password);

Subject subject = SecurityUtils.getSubject();

subject.login(token);

System.out.println("是否登录:"+subject.isAuthenticated());

System.out.println("用户权限是否有VIP权限:"+subject.hasRole("vip"));

if(subject.isAuthenticated()==true){

return new BaseRespMsg(0,"登陆成功");

}

new BaseRespMsg();

return BaseRespMsg.error("登陆失败");

}

/\*

\* 注册

\*/

@RequestMapping("/addUser")

public BaseRespMsg addUser(String username,String password){

Md5Hash md5Hash=new Md5Hash(password);

User user=new User();

user.setUsername(username);

user.setPassword(md5Hash.toString());

user.setState(0);

user.setSalt("cjy");

int isOk = targetService.insert(user);

if(isOk==1){

return new BaseRespMsg(0,"添加成功");

}

return BaseRespMsg.error("添加失败");

}

# 加密加盐

**加盐处理首先在注册和添加用户的时候要对密码进行处理：这里加盐是用的用户名（可以自定，但是用UUID不行，不知道为什么）**

/\*  
 \* 注册  
 \*/  
@RequestMapping("/addUser")  
public BaseRespMsg addUser(String username,String password){  
 User user=new User();  
 user.setUsername(username);  
 user.setPassword(this.makePasswordHasSalt(username,password).toString());  
 user.setState(0);  
 user.setSalt(username);  
 int isOk = targetService.insert(user);  
 if(isOk==1){  
 return new BaseRespMsg(0,"添加成功");  
 }  
 return BaseRespMsg.*error*("添加失败");  
 }  
 /

\*这个是重写shiro给密码加盐的方法从而得到加过盐的密码 SimpleHash的四个参数分别为：加密方式，密码，盐值，加密次数

/  
 public Object makePasswordHasSalt(String username,String password){  
 ByteSource salt = ByteSource.Util.*bytes*(username);  
 Object result = new SimpleHash("MD5",password,salt,1);  
 return result;  
 }

**然后修改自定义realm（MyShiroRealm）的登陆验证方法，在SimpleAuthenticationInfo方法里面加入加盐的参数如**：

authenticationInfo = new SimpleAuthenticationInfo(  
 username, //用户名  
 user.getPassword(), //密码  
 ByteSource.Util.*bytes*(user.getSalt()),//salt=salt  
 getName() //realm name  
 );

# 自定义登陆验证

**创建自定义密码验证登陆类（CustomEncryption）继承HashedCredentialsMatcher类,这里的缓存时间设置为10分钟，最多密码输入错误三次就不让其再登陆**

package com.cjy.shiro.utils;  
  
import org.apache.shiro.authc.AuthenticationInfo;  
import org.apache.shiro.authc.AuthenticationToken;  
import org.apache.shiro.authc.ExcessiveAttemptsException;  
import org.apache.shiro.authc.IncorrectCredentialsException;  
import org.apache.shiro.authc.credential.HashedCredentialsMatcher;  
import org.apache.shiro.cache.Cache;  
import org.apache.shiro.cache.CacheManager;  
  
/\*  
 \* 自定义登陆验密  
 \* cjy  
 \*/  
public class CustomEncryption extends HashedCredentialsMatcher{  
   
 private Cache<String, Integer> cache;  
   
 */\*\*  
 \* 自定义密码错误上限  
 \*/* private Integer retryMax;  
  
  
  
 /\*  
 \* CacheManager缓存管理器  
 \*/  
 public CustomEncryption(CacheManager cacheManager) {  
 cache = cacheManager.getCache("passwordRetryCache");  
 }  
   
 @Override  
 public boolean doCredentialsMatch(AuthenticationToken token, AuthenticationInfo info) throws ExcessiveAttemptsException {  
 String username = (String)token.getPrincipal();  
 Integer retryCount = cache.get(username);  
 if(retryCount == null) {  
 retryCount = new Integer(1);  
 cache.put(username, retryCount);  
 }  
   
   
 if(retryCount > retryMax) {  
 throw new ExcessiveAttemptsException("您已连续错误达" + retryMax + "次！请10分钟后再试");  
 }  
   
 if(cache.getClass().getName().contains("Cache")){  
 cache.put(username, ++retryCount);  
 }  
 //调用父类的校验方法  
 boolean matches = super.doCredentialsMatch(token, info);  
 if(matches) {  
 cache.remove(username);  
 }else {  
  
 throw new IncorrectCredentialsException("您输入的密码已错误" + (retryCount-1) + "次，最多错误" + retryMax + "次");  
 }  
 return true;  
 }  
  
  
 public void setRetryMax(Integer retryMax) {  
 this.retryMax = retryMax;  
 }  
  
 public Integer getRetryMax() {  
 return retryMax;  
 }  
}

**新增一个缓冲处理器的ehcache-shiro.xml文件出来缓冲：**

<?xml version="1.0" encoding="UTF-8"?>  
<ehcache name="es">  
  
 <diskStore path="java.io.tmpdir"/>  
  
 <!--  
 name:缓存名称。  
 maxElementsInMemory:缓存最大数目  
 maxElementsOnDisk：硬盘最大缓存个数。  
 eternal:对象是否永久有效，一但设置了，timeout将不起作用。  
 overflowToDisk:是否保存到磁盘，当系统当机时  
 timeToIdleSeconds:设置对象在失效前的允许闲置时间（单位：秒）。仅当eternal=false对象不是永久有效时使用，可选属性，默认值是0，也就是可闲置时间无穷大。  
 timeToLiveSeconds:设置对象在失效前允许存活时间（单位：秒）。最大时间介于创建时间和失效时间之间。仅当eternal=false对象不是永久有效时使用，默认是0.，也就是对象存活时间无穷大。  
 diskPersistent：是否缓存虚拟机重启期数据 Whether the disk store persists between restarts of the Virtual Machine. The default value is false.  
 diskSpoolBufferSizeMB：这个参数设置DiskStore（磁盘缓存）的缓存区大小。默认是30MB。每个Cache都应该有自己的一个缓冲区。  
 diskExpiryThreadIntervalSeconds：磁盘失效线程运行时间间隔，默认是120秒。  
 memoryStoreEvictionPolicy：当达到maxElementsInMemory限制时，Ehcache将会根据指定的策略去清理内存。默认策略是LRU（最近最少使用）。你可以设置为FIFO（先进先出）或是LFU（较少使用）。  
 clearOnFlush：内存数量最大时是否清除。  
 memoryStoreEvictionPolicy:  
 Ehcache的三种清空策略;  
 FIFO，first in first out，这个是大家最熟的，先进先出。  
 LFU， Less Frequently Used，就是上面例子中使用的策略，直白一点就是讲一直以来最少被使用的。如上面所讲，缓存的元素有一个hit属性，hit值最小的将会被清出缓存。  
 LRU，Least Recently Used，最近最少使用的，缓存的元素有一个时间戳，当缓存容量满了，而又需要腾出地方来缓存新的元素的时候，那么现有缓存元素中时间戳离当前时间最远的元素将被清出缓存。  
 -->  
 <defaultCache  
 maxElementsInMemory="10000"  
 eternal="false"  
 timeToIdleSeconds="120"  
 timeToLiveSeconds="120"  
 overflowToDisk="false"  
 diskPersistent="false"  
 diskExpiryThreadIntervalSeconds="120"  
 />  
  
  
 <!-- 登录记录缓存锁定10分钟 -->  
 <cache name="passwordRetryCache"  
 maxEntriesLocalHeap="2000"  
 eternal="false"  
 timeToIdleSeconds="3600"  
 timeToLiveSeconds="0"  
 overflowToDisk="false"  
 statistics="true">  
 </cache>  
  
</ehcache>

**修改ShrioConfig的实现方法，主要是修改之前的HashedCredentialsMatcher（），securityManager（），myShiroRealm（）方法，并新添加一个缓冲处理器方法ehCacheManager（）**

package com.cjy.shiro.config;  
  
import com.cjy.shiro.utils.CustomEncryption;  
import com.cjy.shiro.utils.MyShiroRealm;  
import org.apache.shiro.authc.credential.CredentialsMatcher;  
import org.apache.shiro.cache.CacheManager;  
import org.apache.shiro.cache.ehcache.EhCacheManager;  
import org.apache.shiro.mgt.SecurityManager;  
import org.apache.shiro.spring.LifecycleBeanPostProcessor;  
import org.apache.shiro.spring.security.interceptor.AuthorizationAttributeSourceAdvisor;  
import org.apache.shiro.spring.web.ShiroFilterFactoryBean;  
import org.apache.shiro.web.mgt.DefaultWebSecurityManager;  
import org.springframework.aop.framework.autoproxy.DefaultAdvisorAutoProxyCreator;  
import org.springframework.beans.factory.annotation.Qualifier;  
import org.springframework.context.annotation.Bean;  
import org.springframework.context.annotation.Configuration;  
import org.springframework.context.annotation.DependsOn;  
  
import java.util.LinkedHashMap;  
  
@Configuration  
public class ShiroConfig {  
 */\*\*  
 \* 密码校验规则HashedCredentialsMatcher  
 \* 这个类是为了对密码进行编码的 ,  
 \* 防止密码在数据库里明码保存 , 当然在登陆认证的时候 ,  
 \* 这个类也负责对form里输入的密码进行编码  
 \* 处理认证匹配处理器：如果自定义需要实现继承HashedCredentialsMatcher  
 \*/* @Bean  
 public CredentialsMatcher credentialsMatcher(CacheManager cacheManager) {  
 CustomEncryption customEncryption = new CustomEncryption(cacheManager);  
 //指定加密方式为MD5  
 customEncryption.setHashAlgorithmName("MD5");  
 //加密次数  
 customEncryption.setHashIterations(1);  
 customEncryption.setStoredCredentialsHexEncoded(true);  
 //密码最对输入错误多少次  
 customEncryption.setRetryMax(3);  
 return customEncryption;  
 }  
  
 */\*\*  
 \* shiro缓存管理器;  
 \* 需要注入对应的其它的实体类中：  
 \* 1、安全管理器：securityManager  
 \* 可见securityManager是整个shiro的核心；  
 \** ***@return*** *\*/* @Bean  
 public EhCacheManager ehCacheManager(){  
 System.*out*.println("ShiroConfiguration.getEhCacheManager()");  
 EhCacheManager cacheManager = new EhCacheManager();  
 cacheManager.setCacheManagerConfigFile("classpath:ehcache-shiro.xml");  
 return cacheManager;  
 }  
  
  
 @Bean  
 @DependsOn("lifecycleBeanPostProcessor")//可选  
 public MyShiroRealm myShiroRealm(CredentialsMatcher credentialsMatcher) {  
 MyShiroRealm myShiroRealm = new MyShiroRealm();  
// myShiroRealm.setAuthorizationCachingEnabled(false);  
 myShiroRealm.setCredentialsMatcher(credentialsMatcher);  
 return myShiroRealm;  
 }  
  
  
 */\*\*  
 \* 定义安全管理器securityManager,注入自定义的realm  
 \** ***@param*** *credentialsMatcher  
 \** ***@return*** *\*/* @Bean  
 public SecurityManager securityManager(CredentialsMatcher credentialsMatcher) {  
 DefaultWebSecurityManager manager = new DefaultWebSecurityManager();  
 manager.setRealm(myShiroRealm(credentialsMatcher));  
 //注入缓存管理器;  
 manager.setCacheManager(ehCacheManager());  
 return manager;  
 }  
  
  
 */\*\*  
 \* 定义shiroFilter过滤器并注入securityManager  
 \** ***@param*** *manager  
 \** ***@return*** *\*/* @Bean  
 public ShiroFilterFactoryBean shiroFilter(@Qualifier("securityManager") SecurityManager manager) {  
 ShiroFilterFactoryBean bean = new ShiroFilterFactoryBean();  
 //设置securityManager  
 bean.setSecurityManager(manager);  
 //设置登录页面  
 //可以写路由也可以写jsp页面的访问路径  
 bean.setLoginUrl("login/html");  
 //设置登录成功跳转的页面  
 bean.setSuccessUrl("/login/index");  
 //设置未授权跳转的页面  
 bean.setUnauthorizedUrl("/login/getopt");  
 //定义过滤器  
 LinkedHashMap<String, String> filterChainDefinitionMap = new LinkedHashMap<>();  
  
 filterChainDefinitionMap.put("/login/index", "authc");  
 filterChainDefinitionMap.put("/login/html", "anon");  
 filterChainDefinitionMap.put("/user/login", "anon");  
 filterChainDefinitionMap.put("/login/getopt", "anon");  
 filterChainDefinitionMap.put("/user/addUser", "anon");  
// filterChainDefinitionMap.put("/admin", "roles[admin]");  
// filterChainDefinitionMap.put("/edit", "perms[delete]");  
// filterChainDefinitionMap.put("/druid/\*\*", "anon");  
 filterChainDefinitionMap.put("/statics/\*\*", "anon");  
 //需要登录访问的资源 , 一般将/\*\*放在最下边  
 filterChainDefinitionMap.put("/\*\*", "authc");  
 bean.setFilterChainDefinitionMap(filterChainDefinitionMap);  
 return bean;  
 }  
  
 */\*\*  
 \* Spring的一个bean , 由Advisor决定对哪些类的方法进行AOP代理 .  
 \** ***@return*** *\*/* @Bean  
 public DefaultAdvisorAutoProxyCreator defaultAdvisorAutoProxyCreator() {  
 DefaultAdvisorAutoProxyCreator creator = new DefaultAdvisorAutoProxyCreator();  
 creator.setProxyTargetClass(true);  
 return creator;  
 }  
  
 */\*\*  
 \* 配置shiro跟spring的关联  
 \** ***@param*** *securityManager  
 \** ***@return*** *\*/* @Bean  
 public AuthorizationAttributeSourceAdvisor authorizationAttributeSourceAdvisor(@Qualifier("securityManager") SecurityManager securityManager) {  
 AuthorizationAttributeSourceAdvisor advisor = new AuthorizationAttributeSourceAdvisor();  
 advisor.setSecurityManager(securityManager);  
 return advisor;  
 }  
  
 */\*\*  
 \* lifecycleBeanPostProcessor是负责生命周期的 , 初始化和销毁的类  
 \* (可选)  
 \*/* @Bean  
 public LifecycleBeanPostProcessor lifecycleBeanPostProcessor() {  
 return new LifecycleBeanPostProcessor();  
 }  
  
}

# 阶段性总结

**学习文档http://www.cnblogs.com/learnhow/p/5694876.html**

**Shiro的核心有SecurityManager，它负责安全认证与授权 Realm，区域可自定义，继承AuthorizingRealm config配置类的方法都要@bean**  **继承类重写方法时多看源码**

# Redis

**Redis 应用场景：缓冲，任务队列，应用排行榜，数据过程处理，网站访问统计，分布式集群架构中的session分离。**

**Jedis是redis的java客户端的开发包**