日历

< 2008年12月 >

日	一	二	三	四	五	六
30	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

常用链接

我的随笔
我的评论
我的参与
最新评论

留言簿(54)

给我留言
查看公开留言
查看私人留言

随笔分类

J2EE学习及探索(8)
Linux和Java(11)
NetBeans与J2ME(6)
SpringSide开发实战(25)
SVN与源代码管理(3)
拥抱Eclipse RCP(7)

随笔档案

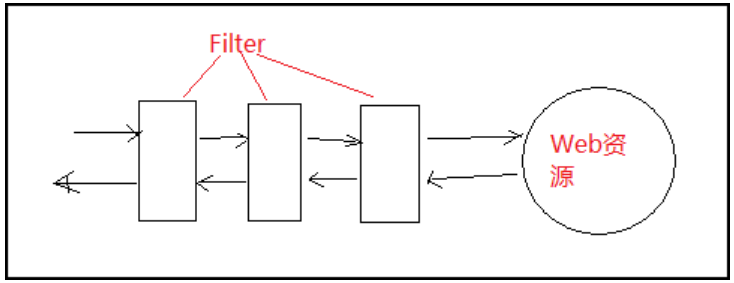
2009年8月 (1)
2009年7月 (6)
2009年5月 (1)
2009年4月 (3)
2009年3月 (1)
2008年12月 (4)
2008年11月 (1)

SpringSide 3 中的安全框架

Posted on 2008-12-07 19:41 海边沫沫 阅读(13441) 评论(15) 编辑 收藏 所属分类: SpringSide开发实战 .

在SpringSide 3的官方文档中，说安全框架使用的是Spring Security 2.0。乍一看，吓了我一跳，以为Acegi这么快就被淘汰了呢。上搜索引擎一搜，发现原来Spring Security 2.0就是Acegi 2.0。悬着的心放下来了。虽然SpringSide 3中关于Acegi的配置文件看起来很不熟悉，但是读了Acegi 2.0的官方文档后，一切都释然了。

先来谈一谈Acegi的基础知识，Acegi的架构比较复杂，但是我希望我下面的只言片语能够把它说清楚。大家都知道，如果要对Web资源进行保护，最好的办法莫过于Filter，要想对方法调用进行保护，最好的办法莫过于AOP。Acegi对Web资源的保护，就是靠Filter实现的。如下图:



一般来说，我们的Filter都是配置在web.xml中，但是Acegi不一样，它在web.xml中配置的只是一个代理，而真正起作用的Filter是作为Bean配置在Spring中的。web.xml中的代理依次调用这些Bean，就实现了对Web资源的保护，同时这些Filter作为Bean被Spring管理，所以实现AOP也很简单，真的是一举两得啊。

Acegi中提供的Filter不少，有十多个，一个一个学起来比较复杂。但是对于我们Web开发者来说，常用的就那么几个，如下图中的被红圈圈标记出来的:

2008年3月 (2)
2008年2月 (3)
2008年1月 (3)
2007年12月 (1)
2007年10月 (3)
2007年9月 (8)
2007年8月 (3)
2007年7月 (2)
2007年3月 (3)
2007年1月 (2)
2006年12月 (5)
2006年11月 (4)
2006年10月 (2)
2006年9月 (1)

收藏夹
我常用的技术资料(6)

我的博客系列
我的 .net 博客
我的 c++ 博客

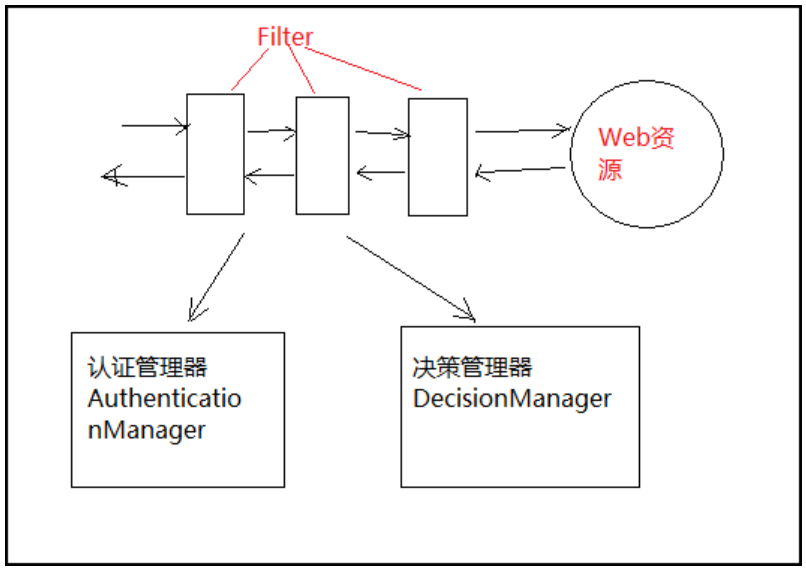
搜索
搜索

积分与排名
积分 - 409476
排名 - 34

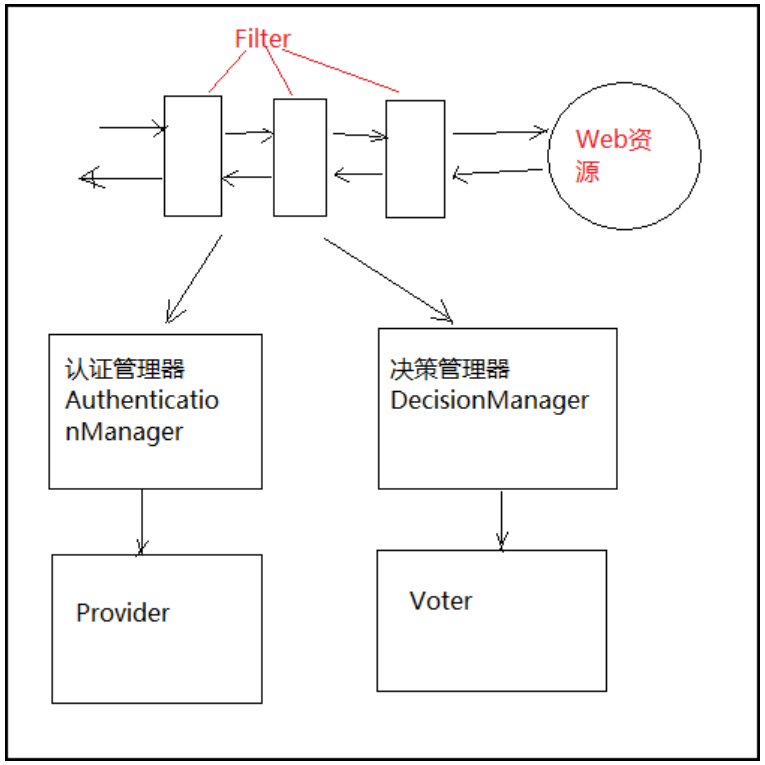
Filter Class
ChannelProcessingFilter
ConcurrentSessionFilter
HttpSessionContextIntegrationFilter
LogoutFilter
X509PreAuthenticatedProcessigFilter
AstractPreAuthenticatedProcessingFilter Subclasses
CasProcessingFilter
AuthenticationProcessingFilter
BasicProcessingFilter
SecurityContextHolderAwareRequestFilter
RememberMeProcessingFilter
AnonymousProcessingFilter
ExceptionTranslationFilter
NtlmProcessingFilter
FilterSecurityInterceptor
SwitchUserProcessingFilter

从上到下，它们实现的功能依次是1、制定必须为https连接；2、从Session中提取用户的认证信息；3、退出登录；4、登录；5、记住用户；6、所有的应用必须配置这个Filter。

一般来说，我们写Web应用只需要熟悉这几个Filter就可以了，如果不需要https连接，连第一个也不用熟悉。但是有人肯定会想，这些Filter怎么和我的数据库联系起来呢？不用着急，这些Filter并不直接处理用户的认证，也不直接处理用户的授权，而是把它们交给了认证管理器和决策管理器。如下图：



对于这两种管理器，那也是不需要我们写代码的，Acegi也提供了现成的类。那么大家又奇怪了：又是现成的，那怎么和我的数据库关联起来呢？别着急，其实这两个管理器自己也不做事，认证管理器把任务交给了Provider，而决策管理器则把任务交给了Voter，如下图：



现在我要告诉你们，这里的Provider和Voter也是不需要我们写代码的。不要崩溃，快到目标了。Acegi提供了多个Provider的实现类，如果我们想用数据库来储存用户的认证数据，那么我们就选择DaoAuthenticationProvider。对于Voter，我们一般选择RoleVoter就够用了，它

最新评论 XML

1. re: 在SpringSide 3 中使用JCaptcha

沫沫您好，请问springside是怎样和JAX-WS集成使用的？能否指点一二？

非常感谢！

--d

2. re: 使用Eclipse RCP进行桌面程序开发（二）：菜单、工具栏和对话框

为什么我在新建工程的时候，如果选择带有intro的插件工程的，自定义的菜单就显示不出来。这个是为什么啊？求博主解答。谢谢！

--kane

3. re: 使用Eclipse RCP进行桌面程序开发（五）：2D绘图

但是加了paintListener之后程序一运行就把四个图像都画出来了，这显然是不合理的啊 怎么解决？

--kane

4. re: 使用SpringSide 3.1.4.3开发Web项目的全过程（上）

好问看看啊

--程序员之家

5. re: 使用Eclipse RCP进行桌面程序开发（三）：视图和透视图[未登录]

评论内容较长,点击标题查看

--小周

阅读排行榜

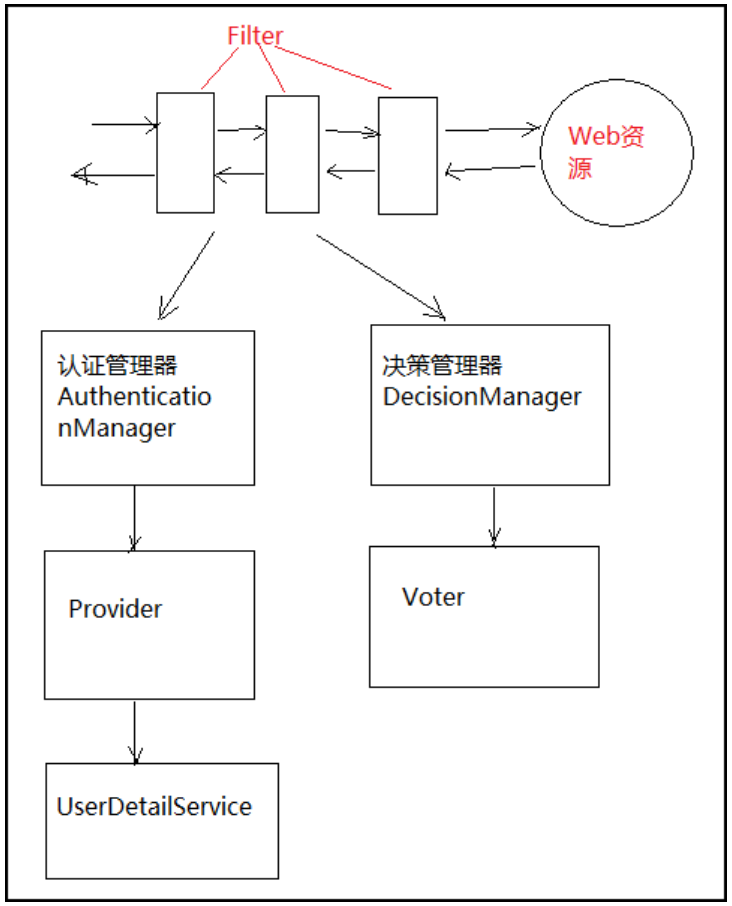
1. 使用Eclipse RCP进行桌面程序开发（一）：快速起步(41354)
2. 使用Eclipse RCP进行桌面程序开发（二）：菜单、工具栏和对话框(20481)
3. 使用Eclipse RCP进行桌面程序开发（三）：视图和透视图(19717)
4. SpringSide 3 的进步(18330)
5. 使用SpringSide 3.1.4.3开发Web项目的全过程（上）(16961)

评论排行榜

1. 使用Eclipse RCP进行桌面程序开发（一）：快速起步(52)
2. SpringSide开发实战（七）：在项目中整合FCKeditor(40)
3. 使用Eclipse RCP进行桌面程序开发（三）：视图和透视图(34)
4. SpringSide 3 的进步(33)
5. 建立一个网站需要多少启动资金？(30)

会根据我们配置文件中的设置来决定是否允许某一个用户访问制定的Web资源。

而DaoAuthenticationProvider也是不直接操作数据库的，它把任务委托给了UserDetailService，如下图：



而我们要做的，就是实现这个UserDetailService。图画得不好，大家不要见笑，但是说了这么多总算是引出了我们开发中的关键，那就是我们要实现自己的UserDetailService，它就是连接我们的数据库和Acegi的桥梁。UserDetailService的要求也很简单，只需要一个返回org.springframework.security.userdetails.User对象的loadUserByUsername(String userName)方法。因此，怎么设计数据库都可以，不管我们是用一个表还是两个表还是三个表，也不管我们是用户-授权，还是用户-角色-授权，还是用户-用户组-角色-授权，这些具体的东西Acegi统统不关心，它只关心返回的那个User对象，至于怎么从数据库中读取数据，那就是我们自己的事了。

反过来再看看上面的过程，我们发现，即使我们要做的只是实现自己的UserDetailService类，但是我们不得不在Spring中配置那一大堆的Bean，包括几个Filter，几个Manager，几个Provider和Voter，而这些配置往往都是重复的无谓的。好在Acegi 2.0也认识到了这个问题，所以，它设计了一个<http>标签，让Acegi的配置得到了简化。下面是SpringSide 3中的配置的截图，大家可以看看：

applicationContext-security.xml | UserDetailServiceImpl.java

```xml
<?xml version="1.0" encoding="UTF-8"?>
<beans:beans xmlns="http://www.springframework.org/schema/security" xmlns:beans="http://www.springframework
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.springframework.org/schema/beans http://www.springframework.org/schema/b
                        http://www.springframework.org/schema/security http://www.springframework.org/schem
    default-autowire="byType" default-lazy-init="true">

    <!-- 在此定义URL与授权的关系.
         注意此处ROLE_*代表的是授权,而非角色.用户、角色、授权及三者关系的数据保存在数据库中. -->
    <http auto-config="true">
        <intercept-url pattern="/login.action*" access="IS_AUTHENTICATED_ANONYMOUSLY" />
        <intercept-url pattern="/user/user!save.action*" access="ROLE_MODIFY_USER" />
        <intercept-url pattern="/user/user!delete.action*" access="ROLE_MODIFY_USER" />
        <intercept-url pattern="/user/user*.action*" access="ROLE_VIEW_USER" />
        <intercept-url pattern="/user/role!save.action*" access="ROLE_MODIFY_ROLE" />
        <intercept-url pattern="/user/role!delete.action*" access="ROLE_MODIFY_ROLE" />
        <intercept-url pattern="/user/role*.action*" access="ROLE_VIEW_ROLE" />
        <form-login login-page="/login.action" default-target-url="/user/user.action" authentication-failur
        <logout logout-success-url="/" />
        <remember-me key="e37f4b31-0c45-11dd-bd0b-0800200c9a66" />
    </http>

    <authentication-provider user-service-ref="userDetailsService">
        <!-- 可设置hash使用sha1或md5散列密码后再存入数据库 -->
        <password-encoder hash="plaintext" />
    </authentication-provider>

    <beans:bean id="userDetailsService" class="personal.youxia.service.security.UserDetailServiceImpl" />
</beans:beans>
```

下图是官方文章中的传统Filter设置和<http>元素之间的对应关系:

Filter Class	Namespace Element or Attribute
ChannelProcessingFilter	http/intercept-url
ConcurrentSessionFilter	http/concurrent-session-control
HttpSessionContextIntegrationFilter	http
LogoutFilter	http/logout
X509PreAuthenticatedProcessigFilter	http/x509
AstractPreAuthenticatedProcessingFilter Subclasses	N/A
CasProcessingFilter	N/A
AuthenticationProcessingFilter	http/form-login
BasicProcessingFilter	http/http-basic
SecurityContextHolderAwareRequestFilter	http/@servlet-api-provision
RememberMeProcessingFilter	http/remember-me
AnonymousProcessingFilter	http/anonymous
ExceptionTranslationFilter	http
NtlmProcessingFilter	N/A
FilterSecurityInterceptor	http
SwitchUserProcessingFilter	N/A

下面的代码是SpringSide 3中实现UserDetailService的范例，在SpringSide 3的范例中，白衣使用了三个表User、Role、Authority。但是Acegi不关心你用了几个表，它只关心UserDetails对象。而决定用户能否访问指定Web资源的，是RoleVoter类，无需任何修改它可以工作得很好，唯一的缺点是它只认ROLE_前缀，所以搞得白衣的Authority看起来都象角色，不伦不类。

```
package personal.youxia.service.security;

import java.util.ArrayList;
import java.util.List;

import org.springframework.beans.factory.annotation.Required;
import org.springframework.dao.DataAccessException;
import org.springframework.security.GrantedAuthority;
import org.springframework.security.GrantedAuthorityImpl;
import org.springframework.security.userdetails.UserDetails;
import org.springframework.security.userdetails.UserDetailsService;
import org.springframework.security.userdetails.UsernameNotFoundException;
import personal.youxia.entity.user.Authority;
import personal.youxia.entity.user.Role;
import personal.youxia.entity.user.User;
import personal.youxia.service.user.UserManager;

/**
```

```
 * 实现SpringSecurity的UserDetailsService接口,获取用户Detail信息.
 *
 * @author calvin
 */
public class UserDetailServiceImpl implements UserDetailsService {

    private UserManager userManager;

    public UserDetails loadUserByUsername(String userName) throws UsernameNotFoundException, DataAccessException {
        User user = userManager.getUserByLoginName(userName);
        if (user == null)
            throw new UsernameNotFoundException(userName + " 不存在");

        List<GrantedAuthority> authsList = new ArrayList<GrantedAuthority>();

        for (Role role : user.getRoles()) {
            for (Authority authority : role.getAuths()) {
                authsList.add(new GrantedAuthorityImpl(authority.getName()));
            }
        }

        // 目前在MultiDatabaseExample的User类中没有enabled, accountNonExpired,credentialsNonExpired, accountNonLocked等属性
        // 暂时全部设为true,在需要时才添加这些属性.
        org.springframework.security.userdetails.User userdetail = new org.springframework.security.userdetails.User(
                user.getLoginName(), user.getPassword(), true, true, true, true, authsList
                        .toArray(new GrantedAuthority[authsList.size()]));

        return userdetail;
    }

    @Required
    public void setUserManager(UserManager userManager) {
        this.userManager = userManager;
    }
}
```

最后再来说说这个命名的问题，我对Authentication和Authority这两个单词比较反感，两个原因，一是因为它们太生僻了，二是因为它们长得太像了，明明一个是认证，一个是授权，意思相差很远，外貌却如此相似，确实很烦人。如果让我来选择，我喜欢Privilege这个单词，在我刚使用MySQL的时候就跟它很熟了，所以在我的项目中，我可能会用Privilege来代替Authority。如果我们只使用User-Role两级关系，使用RoleVoter默认的ROLE_前缀当然没有关系，如果是像白衣这样是用三层关系，最好还是把这个前缀改一改，以免混淆。

评论

 # re: SpringSide 3 中的安全框架 回复 更多评论
2008-12-08 10:15 by 杨爱友

以前看过这个安全框架，觉得配置太复杂，放弃使用了，今天叫你说的这么简单，回头再看一下。

 # re: SpringSide 3 中的安全框架 回复 更多评论
2008-12-08 11:12 by regale

谢谢!

 # re: SpringSide 3 中的安全框架 回复 更多评论
2008-12-08 11:17 by leekiang

挺奇怪的，权限的前缀为什么要用"ROLE_"呢，我觉得用"PRIVILEGE_"或者"AUTHORITY_"比较恰当。

 # re: SpringSide 3 中的安全框架 回复 更多评论
2008-12-08 20:11 by 火线生存

讲得非常通俗，对Spring Security又理解一层了。非常感谢!

 # re: SpringSide 3 中的安全框架 回复 更多评论
2008-12-10 08:46 by 淘声依旧

简单多了

 # re: SpringSide 3 中的安全框架 回复 更多评论
2008-12-11 22:33 by 有点不明白!

这些是简化了配置，不过我还是不明白， 如何把 所有的权限和角色都定义在数据库中，常常在开发中 角色是可以维护的， 而且 较大的项目 权限这样配置工作量太大。有没有什么好的办法。

 # re: SpringSide 3 中的安全框架 回复 更多评论
2008-12-24 13:15 by 海边沫沫

补充:

前文所讲的是我对Acegi的一些理解，我认为只有把条理搞清楚了，才更容易深入。我想得比较简单，当然会漏掉一些细节。这里把它补充一下。

1、我上面讲到的主要内容，包含了认证和授权，但是漏掉了资源，资源就是我们需要保护的URL，或者一些类中的方法。要保护URL，在xml文件中按照前面的例子配置就可以了，要保护类中的方法，使用@secured就可以了。
但是它们是和Acegi中的哪个组件关联起来的呢？是FilterSecurityInterceptor和MethodSecurityInterceptor，这两个Interceptor都需要设置一个叫objectDefinitionSource的属性。所以，有人要问，如何把对资源的保护设置全部转移到数据库中，避免写在xml中，那就要从这个objectDefinitionSource着手了。

2、前面讲到了UserDetailService，事实上在Acegi中还需要配置别的Service，如RememberMeService，当然，该Service也是现成的，不需要我们写代码的，RememberMeProcessingFilter需要依赖这个Service。

3、Acegi支持OpenID和CAS 3，这两个东西是干什么的呢？是可以实现单点登录功能的，也就是允许用户只登录一次，就可以使用多个网站。这对于那些很庞大的网站非常有用，可以把用户登录这样的操作集中在一台服务器上。要使用CAS，只需要配置Filter时选择CASProcessingFilte，配置Provider时选择CasAuthenticationProvider，其余的概念都是相通的。具体的实现细节，大家慢慢摸索吧。

 # re: SpringSide 3 中的安全框架 回复 更多评论
2008-12-24 15:44 by 虎啸龙吟

讲的比较清楚、透彻！但有几个问题:
IS_AUTHENTICATED_ANONYMOUSLY、ROLE_MODIFY_USER等 有什么作用？由谁定义啊？

 # re: SpringSide 3 中的安全框架 回复 更多评论
2008-12-24 20:16 by 海边沫沫

@虎啸龙吟
这些是我们自己定义的。用户、角色、授权都是开发者自己定义的，在SpringSide中，这些东西是用数据库保存的，而资源和授权的关系，是定义在xml文件中的，就是你看到的配置文件的内容。

 # 沫沫帮忙看看这个文题吧，帮忙解决一下吧 回复 更多评论
2009-01-06 16:45 by playingfly

沫沫帮忙看看这个文题吧，也是关于安全认证登陆的，帮忙解决一下吧 ，十分感谢了！！！

http://forum.springside.org.cn/viewthread.php?tid=3352&extra=page%3D1

 # re: SpringSide 3 中的安全框架 回复 更多评论
2009-01-12 19:18 by 江南白衣

ROLE_的前缀，貌似不大容易改掉啊，谁改过的告诉一下方法，的确很容易让人混淆。

 # re: SpringSide 3 中的安全框架 回复 更多评论
2009-01-13 16:58 by yzl45

在这里要强调一点，acegi已经不存在了，在1.0X以后，就叫做Spring Security了，这个是官方的正式更名。
“ROLE_”这个前缀是Spring Security一个默认的前缀，如果不想用，可以替换它，提换的方法是:

```
<beans:bean id="accessDecisionManager" class="org.springframework.security.vote.AffirmativeBased">
<beans:property name="allowIfAllAbstainDecisions" value="false"/>
<beans:property name="decisionVoters">
<beans:list>
<beans:bean class="org.springframework.security.vote.RoleVoter">
<beans:property name="rolePrefix" value="替换成你想要的前缀"></beans:property>
</beans:bean>
<beans:bean class="org.springframework.security.vote.AuthenticatedVoter"/>
</beans:list>
</beans:property>
</beans:bean>
```

 # re: SpringSide 3 中的安全框架[未登录] 回复 更多评论
2009-01-14 00:20 by 江南白衣

SpringSide的SVN里ROLE_已经改成AUTH_了 ： ）

 # re: SpringSide 3 中的安全框架 回复 更多评论

2009-02-01 11:22 by mojiezhong

实现“用户-用户组-角色-授权”四级关系与“用户-角色-授权”关系难度大吗？性能影响如何？

 # re: SpringSide 3 中的安全框架 回复 更多评论
2009-05-08 16:00 by 小k

很久以前试用了一下acegi1.x版本,,用户 角色== 信息都放数据库里面来,,

但是问题来了.我想做动态权限,这个玩意是使用别人的系统的时候看到的...

如果使用的acegi 但标签字页面控制了显示,那么还有办法让角色也动态么??

新用户注册 刷新评论列表

博问 - 解决您的IT难题

博客园 博问 IT新闻 Java程序员招聘

标题 re: SpringSide 3 中的安全框架

姓名

主页

验证码 * 1195

内容(请不要发表任何与政治相关的内容)

Remember Me?

提交 登录

[使用Ctrl+Enter键可以直接提交]

IT新闻:

· 10幅图让你了解Google与其它科技公司的不同之处

· Zynga或将与微软结盟 进军电视游戏领域

· RIM非洲开拓新市场 拟推出更低价格手机

· 六款优秀的Linux吉他工具

· 当当网俞渝呼吁政府应在网购立法上有所作为

博客园首页随笔:

· UMDF驱动程序快速上手

· C# 温故而知新：Stream篇（三）

· 微软官方windows phone开发视频教程第一天视频(附下载地址)

· 用原生JS进行CSS格式化和压缩

· Sql正则替换

知识库:

· Windows Runtime - 面向对象化的C++（并非意味着托管）

· 谈一谈 Windows 8 的软件开发架构

· 开发Metro版浏览器

· 开发WinRT自定义组件

· Win8探索学习笔记

网站导航:
博客园 IT新闻 知识库 C++博客 程序员招聘 管理
相关文章:
在SpringSide 3 中使用JCaptcha
使用SpringSide 3.1.4.3开发Web项目的全过程（下）
使用SpringSide 3.1.4.3开发Web项目的全过程（中）
使用SpringSide 3.1.4.3开发Web项目的全过程（上）
在SpringSide 3 中使用多个数据库的方法
SpringSide 3 中的多数据源配置的问题
SpringSide 3 中的数据库访问层
使用Fedora 10 进行Java开发，发两张截图让大家尝尝鲜
SpringSide 3 中的 Struts 2