昵称：坚持很贵
园龄：3年10个月
粉丝：7
关注：10
+加关注

< 2016年11月 >

日	一	二	三	四	五	六
30	31	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	1	2	3
4	5	6	7	8	9	10

搜索

找找看

谷歌搜索

常用链接

我的随笔

我的评论

我的参与

最新评论

我的标签

我的标签

MyBatis(4)

缓存(3)

aop(2)

日志(2)

spring(2)

Dbutils(2)

JDBC(2)

Jdk(1)

JGroups(1)

Jmock(1)

REST API权限集成设计

REST API权限集成设计

应用分为两大部分，前端**html+**后端**Rest**服务，前端**html**和后端**Rest**服务部署完全分离。
目标：可访问资源都处于权限控制之下**(**意味着通过浏览器地址栏的任意**url**都会被拦截**)**，并提供跨域访问支持。
***

项目模块

前端模块：应用界面，通过**rest**接口与后台交互。
后端模块：**UPM(**用户权限管理**)**模块**+**数据服务**(**包含多种数据来源，比如本地**DB**、第三方服务等**)**统一作为**Rest**封装层。

应用模块权限访问交互流程

Token

- **Client**和**Server**交互的令牌，相当于客户端和**Server**交互的唯一**id**，绝大部分**(**登录时不需要**)Client**请求都会带上此**id**，和**SessionId**类似，只是它不必受限于单个**Web**容器并能够自定义**Token**的过期时间、生成策略。
- 对于一个独立用户，**Server**和**UPM**共用相同的**Token**。
- **Token**包含**tokenid+userid+**其它辅助信息**.**

UPM

UPM提供对整个应用系统中关于资源和用户角色关系的权限配置，并且对外提供认证和授权的接口。

Token Manager

维护**Token**生命周期，可配置**Token**的过期时间，**Token Mananger**维护一张**hash**表，**k**为用户**id**，**v**为**Token**，每次用户请求匹配**token**时自动检查**Token**是否过期，如果过期，则返回过期的状态码。
Token指标：**Token**使用次数、**Token**过期时间
Token使用次数：如果客户端请求次数大于了**Token**默认设定请求次数，则需要重新生成**Token**，但无需重新登录。
Token过期时间：超过**Token**过期时间的请求将会触发重新登录。

登录权限交互流程

业务流：用户登录**(login.html)**访问，输入用户名和密码后访问主页**(index.html)**

更多

随笔分类

CI(1)

Core Java(4)

J2EE体系(7)

Life

Linux(2)

WebService相关(1)

测试开发(2)

分布式(5)

工具代码(3)

权限设计相关(1)

通信(1)

随笔档案

2015年11月 (9)

2015年10月 (4)

2015年9月 (3)

2015年7月 (2)

2014年11月 (2)

2014年10月 (3)

2014年9月 (2)

2013年2月 (1)

2012年12月 (2)

相册

技术图例(3)

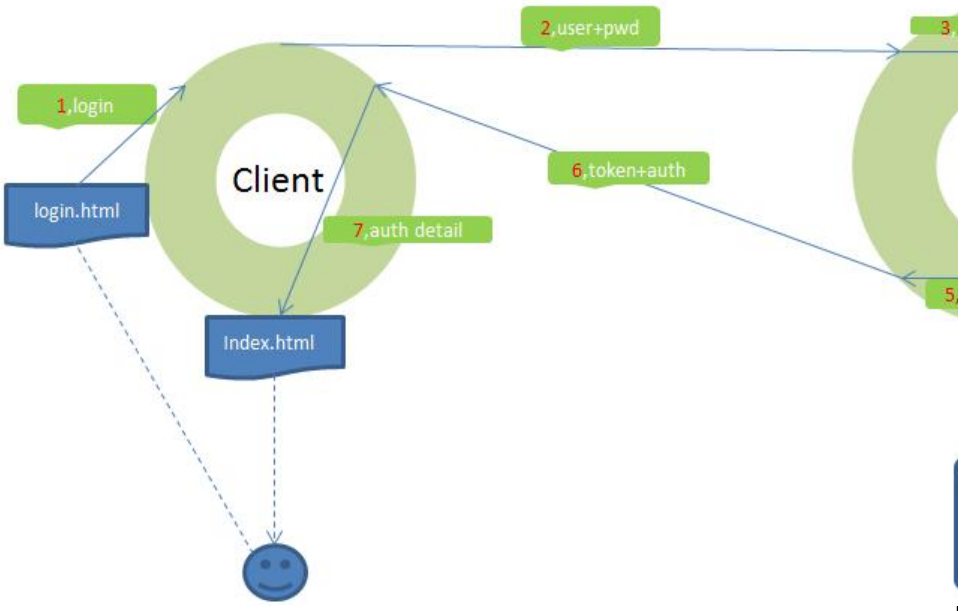
最新评论

1. Re:Java序列化技术与Protobuff

楼主ProtostuffSerializerUtil给我也发一份，谢谢
350967791@qq.com

--hcb

登录权限交互流程：



- 用户访问**Client**静态资源**login.html**，填写用户名和密码并执行登录
- 用户名和密码被传递到**UPM**
- **UPM**执行认证**(authentication)**，校验用户名和密码
- 认证通过后执行授权**(authorization)**，获取和当前用户关联的所有可访问的资源
- 如果上一步执行成功，**UPM**将请求**TokenManager**创建**Token**，若不通过则返回错误码**(**授权、认证错误码不同**)**
- **UPM**将**token+**授权数据返回给客户端
- 客户端收到**token+**授权数据展现**index.html**给用户**(index.html**可能存在多个模块**,**需要控制页面展示**)**

备注：**Client**端需要处理从**UPM**端返回的数据，包含**Token**和状态码，如果状态码不是成功标识，依据具体的状态码转向特定页面，否则登录成功，存储**Token(**比如存储到**Cookie)**，并跳转到首页。

登录后资源访问

业务流：假定用户进入**index.html**存在一个**rest**资源链接，对应**rest**服务**"/audience/report"**，用于请求最新的人群报告，人群报告展示页面为**audience.html**

备注：此时用户已登录，**Client**的**Cookie**中已存在**Token**

2. Re:Spring BeanPostProcessor与动态加载数据源配置

我刚刚你的方式试，但是我再查询的时候还是走了**xml**配置文件。**java.lang.ClassNotFoundException: ******

--遁世思伊

3. Re:Protostuff序列化工具类

不知道博主是否遇到 序列化数字时数字大小操作正负**128** 就会出错的问题？

--Lone|yBoy

4. Re:REST API权限集成设计

如果**token** 被截获，是不是导致了可以随意访问

--damozhiying110

5. Re:Java序列化技术与**Protobuff**

楼主也发我一份吧，谢谢啦，**1798761638@qq.com**

--bigmice

阅读排行榜

1. Java 异步处理简单实践**(20972)**

2. Spring Security3初步学习**(16230)**

3. Java基础数据类型二进制转换**(13121)**

4. Java序列化技术与**Protobuff(6329)**

5. JGroups 入门实践**(5505)**

评论排行榜

1. Java序列化技术与**Protobuff(9)**

2. Java 异步处理简单实践**(3)**

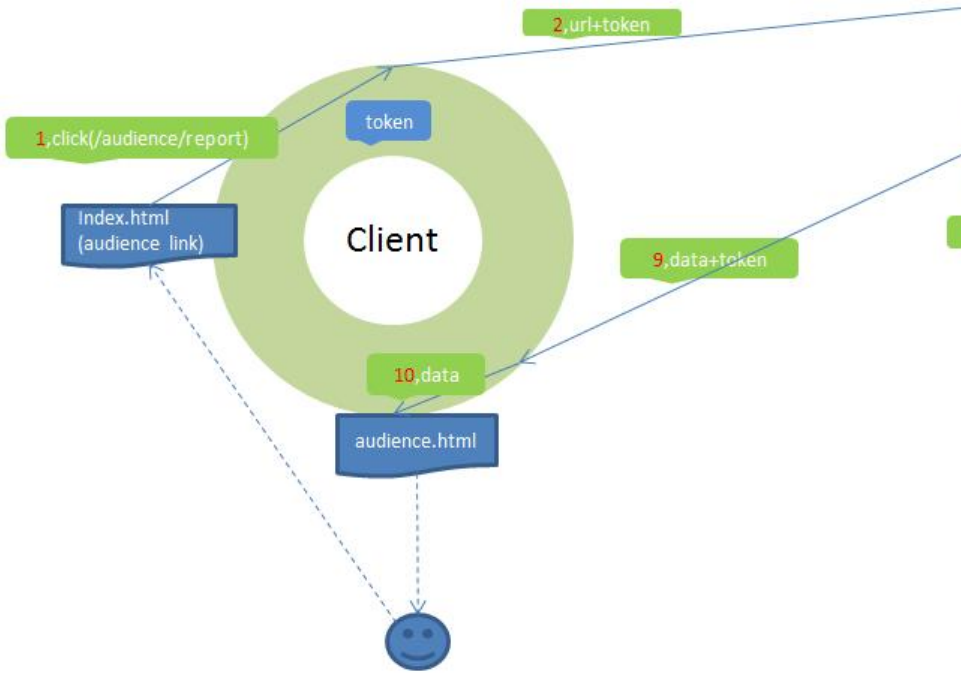
3. Spring BeanPostProcessor与动态加载数据源配置**(1)**

4. Protostuff序列化工具类**(1)**

5. REST API权限集成设计**(1)**

推荐排行榜

人群报告权限交互流程：



- 用户点击"人群报告"链接**(rest url=/audience/report)**
- 客户端发送请求**(**包含**user+rest url+ token)**给**UPM**
- 客户端发送请求**(rest url=/audience/report + token)**发给**Server**
- **Server**匹配**token**，**UPM**授权**rest url**，如果**token**未过期并且匹配成功并且**upm**授权成功将调用实际业务处理流获取数据，否则返回错误码
- 将数据和**Token**信息返回给客户端
- **Client**依据**Server**的数据渲染人群报告页面展现给用户

前后端交互备注

- 前端的所有请求，除登入请求之外，其它所有请求都在**header**中附带用户**id(userId)**和令牌**(tokenId)**传递给服务端。
- 任何请求都必须带令牌，若无令牌，直接**rest url**访问目标资源，则返回登录页。

一段旅程，远去所有昨天的昨天，如记事本翻开新的一页，永远的不漏痕迹的把记忆藏在一片洁白中。然后绚烂的开始新的故事。

分类：权限设计相关

标签：**REST**，权限

坚持很贵
关注 - 10
粉丝 - 7
+加关注

0 0

« 上一篇：轻量级封装**DbUtils&Mybatis**之四**MyBatis**主键
» 下一篇：**MongoDB**入门实践

posted @ 2015-11-26 11:57 坚持很贵 阅读**(1354)** 评论**(1)** 编辑 收藏

评论列表

#1楼 2016-04-12 14:45 damozhiying110

如果token 被截获，是不是导致了可以随意访问

支持(0) 反对(0)

刷新评论 刷新页面 返回顶部

注册用户登录后才能发表评论，请 登录 或 注册，访问网站首页。

最新IT新闻:
· 13岁的京东和13岁的亚马逊
· 都说政府项目钱多又好干！富士通哭着对你说，童话里都是骗人的...
· 并购携程去哪儿公寓民宿业务后 途家进行重大组织架构调整
· 三星收购Viv 加入语音助手大战
· 小米想让Note 2成为杀招 但这些因素或许会让它落空
» 更多新闻...

最新知识库文章:
· 循序渐进地代码重构
· 技术的正宗与野路子
· 陈皓：什么是工程师文化？
· 没那么难，谈CSS的设计模式
· 程序猿媳妇儿注意事项
» 更多知识库文章...