

JEECG 智能开发平台

平台权限实战开发手册 V3.7.2

2017/12/07

www.jeecg.org

Jeecg 社区

目 录

1. 权限概念.....	4
1.1. 功能简述.....	4
1.2. 基本概念.....	5
1.3. 权限模型.....	5
1.4. 权限技巧.....	5
2. 权限对象.....	6
2.1. 用户管理.....	6
2.2. 角色管理.....	6
2.3. 菜单管理.....	7
2.4. 组织机构管理.....	7
3. 列表按钮权限控制.....	8
3.1. 按钮权限规则说明.....	8
3.2. 按钮权限页面编码实现.....	8
3.3. 按钮权限配置.....	9
3.4. 按钮权限控制效果.....	10
3.5. 按钮权限授权效果.....	10
4. 页面表单权限控制.....	11
4.1. 表单权限规则说明.....	11
4.2. 表单权限标签介绍.....	12
4.3. 表单权限页面编码实现.....	13
4.3.1. 邮箱字段隐藏 t:authFilter.....	13
4.3.2. 手机号字段隐藏 t:hasPermission.....	14
4.3.3. 金额字段禁用 t:authFilter.....	15
4.4. 表单权限配置.....	16
4.5. 表单权限控制效果.....	16
4.6. 表单权限授权效果.....	17
5. 列表数据权限控制.....	18
5.1. 功能说明.....	18

5.2.	数据权限控制模式	18
5.3.	数据权限规则篇	19
5.3.1.	当前用户上下文变量	19
5.3.2.	建表规范（系统标准字段）	19
5.3.3.	组织机构邮编规则	19
5.4.	案例一（行级别 - 限制 demo 用户不能看 admin 的数据）	20
5.4.1.	数据权限案例	20
5.4.2.	数据权限菜单配置	20
5.4.3.	数据权限控制规则配置	21
5.4.4.	数据权限授权角色	23
5.4.5.	测试数据权限效果	24
5.5.	案例二（行级权限 - 登录人只能看自己数据）	24
5.5.1.	数据权限案例	24
5.5.2.	数据权限规则配置	25
5.5.3.	数据权限授权角色	26
5.5.4.	测试数据权限效果	26
5.6.	案例三（行级权限 - 登录人可看下级所有人数据）	27
5.6.1.	数据权限案例	27
5.6.2.	数据规则配置原理	27
5.6.3.	基础数据准备	27
5.6.4.	数据权限规则配置	28
5.6.5.	数据权限授权角色	29
5.6.6.	测试数据权限效果	29
5.7.	案例四（列级别权限 - 不同的人看到数据列表不同的列）	30
5.7.1.	功能说明	30
5.7.2.	列级别权限案例	30
5.7.3.	列表页面编码规则	30
5.7.4.	列表行权限控件配置	30
5.7.5.	列表行数据权限授权角色	32
5.7.6.	测试列表行数据权限效果	32

5.8.	采用 Minidao 方式权限集成.....	32
5.8.1.	权限配置规则	32
5.8.1.	权限生成 SQL 规则获取方法.....	33

1. 权限概念

1.1. 功能简述

JEECG 封装完善的用户权限模块，支持菜单权限，列表按钮权限，表单字段权限、数据权限等。数据权限功能已实现极致：支持行级、列级、字段级控制，实现不同人看不同数据，不同人对同一个页面操作不同字段。系统按钮权限和表单权限原来是正控制，只有授权的人才有权限，未授权看不到对应按钮；（admin 拥有超级权限，不受控制）

场景举例： 销售经理可以看下属所有销售人员的数据，销售人员只能看自己的数据。

1.2. 基本概念

权限管理模块涉及到的对象有：用户、角色、组织机构和系统资源(包括系统菜单、页面控件、数据资源等)。系统资源以角色为单位进行管理，用户可以拥有多个角色，角色可以被分配给多个用户；组织机构也可以分配多个角色，机构下的人自动继承相关角色。而权限的意思就是对某个资源的某个操作。一般通用的权限管理模块规定：所谓资源即应用系统中提供的要进行鉴权才能访问的资源(比如各类数据, 系统菜单)；所谓操作即增加、修改、删除、查询等操作。

1.3. 权限模型

用户权限模型，指的是用来表达用户信息及用户权限信息的数据模型。即能证明“你是谁？”、“你能访问哪些受保护资源？”。

用户与角色之间构成多对多关系。表示同一个用户可以拥有多个角色，一个角色可以被多个用户所拥有。

角色与资源之间构成多对多关系。表示同一个资源可以被多个角色访问，一个角色可以访问多个资源。

1.4. 权限技巧

1. 权限拦截排除注解JAuth

```
@JAuth(auth=Permission.SKIP_AUTH)
```

具体用法:

[1]. 类注解表示该类下所有请求直接通过权限url拦截器

[2]. 方法注解表示该方法的请求直接通过权限url拦截器

2. 权限拦截支持请求URL(目前支持带一个参数, 但格式有要求, 不能带等号)

```
loginController.do?login
```

```
loginController.do, 不支持模式: loginController.do?name=2
```

3. admin 拥有超级权限, 不受按钮权限和表单权限控制。

4. 清理垃圾权限配置 SQL 脚步

```
delete from t_s_role_function where functionid not in(select id from t_s_function)
```

2. 权限对象

JEECG 权限设计，采用用户、角色、菜单、组织机构来进行组建，角色为主要授权对象，组织机构可以分配角色。

菜单类型分两种：权限类型和菜单类型

- 菜单类型： 菜单类型的菜单，在首页菜单展示和访问使用
- 权限类型： 权限类型的菜单，在首页菜单不做展示，只做权限控制使用

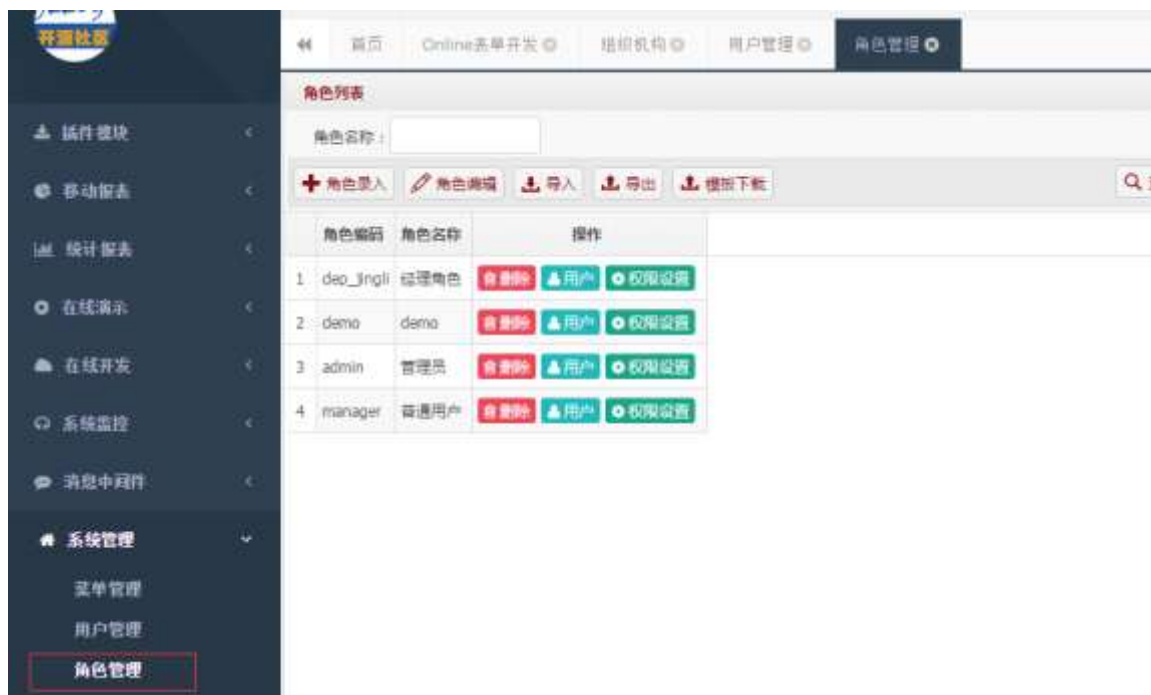
2.1.用户管理

用户管理，用户可以分配多个角色；也可以隶属于多个组织机构，多个组织机构情况下，登录需要选择机构登录，方便数据权限控制；

	用户账号	用户名称	组织机构	角色	创建时间	状态	
1	demo	demo	销售人员,	demo	2015-05-21	激活	自删除
2	scott	张代浩	销售人员,	普通用户	2016-03-17	激活	自删除
3	lisi	李四	销售经理,	经理角色	2016-03-17	激活	自删除
4	admin	管理员	JEECG开源社区,	管理员	2016-07-20	激活	自删除
5	cgspy	采购审批员	中国人寿总公司,	管理员	2016-09-30	激活	自删除

2.2.角色管理

角色是权限组单位，通过角色管理菜单权限。



2.3. 菜单管理

菜单管理，用来做首页菜单管理和权限管理，权限包括：菜单访问权限、按钮权限、表单权限、数据权限。



2.4. 组织机构管理

组织机构管理，支持集团模式多个分公司，第一级默认是公司类型，从二级开始可设置部门和岗位，部门和岗位通过类型区分；组织机构可以单独设置角色；



3. 列表按钮权限控制

3.1. 按钮权限规则说明

列表按钮权限控制，主要是控制列表上按钮、操作链接的隐藏；按钮权限配置后，默认未授权用户都看不到，只有赋权后才能看到（**admin 除外**）。

控制精度：列表按钮\链接的权限控制，统一采用隐藏方式实现（不区分：隐藏\禁用）。

控制方式：配置权限标签参数 `operationCode`（采用 UI 标签）。

3.2. 按钮权限页面编码实现

通过设置权限 `code` 来实现，列表按钮或链接增加权限参数：`operationCode="copyOnlineTable"`；

目前的设计是配置上权限标签参数后就开始受权限控制，所有人都看不到。

```
<t:dgFunOpt funname="copyOnline(id)" title="复制表单" operationCode="copyOnlineTable" urlclass="ace_button"
urlfont="fa-copy"></t:dgFunOpt>

<t:dgToolBar title="form.generate" icon="icon-add" url="cgformTransController.do?trans"
operationCode="db_generate_form" funname="addToData"></t:dgToolBar>

<t:dgFunOpt funname="delCgForm(id)" operationCode="delCgForm" title="删除" ></t:dgFunOpt>
```


3.3. 按钮权限配置

针对菜单请求地址 `cgFormHeadController.do?cgFormHeadList`，配置对应的按钮权限。

注意：请求 URL 有一定的规则要求（目前 URL 只支持带一个参数，且格式有要求，不能带等号），

例如：`loginController.do?login`，不支持等号模式：`loginController.do?name=2`

① 菜单对应按钮权限列表



② 按钮权限配置

说明：页面控件编码配置规则对应，标签参数 `operationCode` 值（规则类型不区分）。



3.4. 按钮权限控制效果

通过按钮权限配置，限制未授权用户访问菜单【Online 表单开发】，没有按钮[数据库导入表单][复制表单] 的操作权限。

[1]、原页面效果如下：



[2]、权限控制效果如下：

通过截图发现，两个按钮[数据库导入表单]、 [复制表单]，已经成功隐藏。



3.5. 按钮权限授权效果

[1]、角色授权

按钮权限配置后，默认未授权用户都看不到，只有赋权后才能看到，此时给 demo 角色授权，测试是否可看到对应的按钮。



[2]、授权效果确认

授权成功后，采用 demo 用户登录系统，访问菜单“Online 表单开发”效果如下，[数据库导入表单][复制表单] 按钮成功显示。



4. 页面表单权限控制

4.1. 表单权限规则说明

页面表单权限，主要用来控制一个页面上控件或者代码块的隐藏和禁用。表单权限配置后，默认非授权用户都受控制，只有赋权才解除控制（admin 除外）。

控制精度：禁用（只读不可写）、隐藏（不可读）。

控制方式：有两种方式，分别对应两个标签，具体用法看表单权限标签介绍。

常见误区：

针对页面表单进行权限控制，大家经常把 URL 配置错误，错以为是 list 页面，注意应该是需要控制的页面请求。

例如：`jeecgListDemoController.do?goAdd`

4.2. 表单权限标签介绍

表单权限控制，通过权限标签实现，两种标签两种不同使用方式。

表单权限智能标签	<code><t:authFilter /></code>
用法:	<p>将该标签放在 JSP 页面最底部即可，不要采用包含写法</p> <p>规则: 采用 Jquery 思路，用 JS 方式对页面控件进行控制</p> <p>页面控件编码，规则如下：</p> <p>#id => 表单控件 ID</p> <p>.class => 表单控件样式</p> <p>控制精度: 可控制表单片段的隐藏和禁用</p>
表单权限包含标签	<pre><t:hasPermission code="add"> <input name="mobile" class="inputxt" value="{depart.mobile }"/> </t:hasPermission></pre>
用法:	<p>采用包含的方式：</p> <p>code 对应页面控件权限的 [页面控件编码]</p> <p>规则: 包含权限标签，包含的表单代码片段，会通过 code 权限匹配，匹配成功，页面片段将不显示；</p> <p>控制精度: 只能控制表单片段的隐藏（不区分隐藏和禁用）</p>

`<t:authFilter />` 标签用法例子:

类似 jquery 语法（规则如下）：

- `#id => #mail_id`（通过 ID 控制页面控件的权限）
- `.class => .form`（通过 class 控制页面控件的权限）

参考例子:

语法一: `#add_phnoe`

```
<tr id= "add_phnoe">
  <td align="right" nowrap><label class="Validform_label"> 手机号码: </label></td>
  <td class="value"><input class="inputxt" name="mobilePhone"
value="{jgDemo.mobilePhone}" datatype="m" errorMsg="手机号码不正确!" ignore="ignore">
  <span class="Validform_checktip"></span></td>
</tr>
```

语法二: `.add_phnoe class`

```
<tr class= "add_phnoe">
```

```

<td align="right" nowrap><label class="Validform_label"> 手机号码: </label></td>
<td class="value"><input class="inputxt" name="mobilePhone"
value="{jgDemo.mobilePhone}" datatype="m" errmsg="手机号码不正确!" ignore="ignore">
<span class="Validform_checktip"></span></td>
</tr>
    
```

4.3. 表单权限页面编码实现

4.3.1. 邮箱字段隐藏 t:authFilter

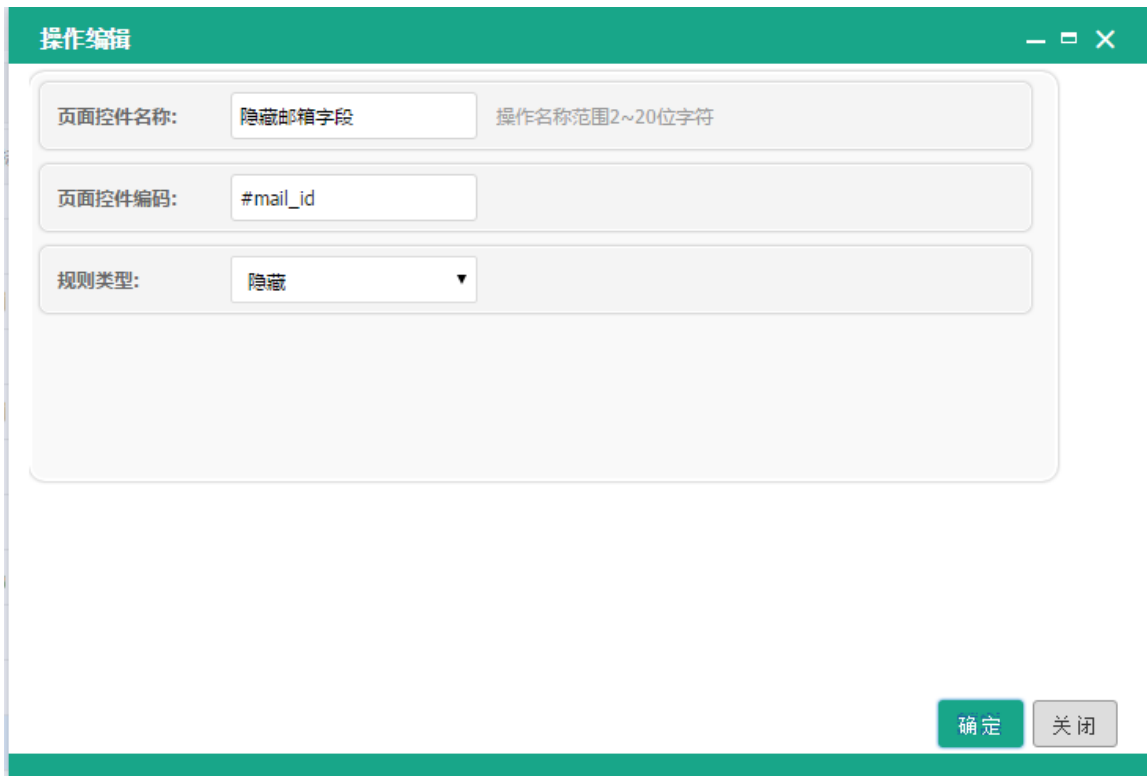
说明： 邮箱字段隐藏，采用权限标签<t:authFilter />实现，authFilter 标签是一个权限智能标签，放在需要控制的页面底部即可（非包含用法）；

[1]、邮箱字段控制隐藏，编码如下

```

62 <input name="shoppingSite" class="form" id="shoppingSite" type="checkbox" value="3" /> 选4)
63 <span class="Validform_checktip"></span>
64 </div>
65
66
67 <div class="form" id="mail_id">
68 <label class="Validform_label"> 邮箱: </label>
69 <input type="text" name="demoorder" id="demoorder" datatype="e" errmsg="邮箱非法">
70 <span class="Validform_checktip"></span>
71 </div>
72
73 <t:hasPermission code="phone_code">
74 <div class="form">
75 <label class="Validform_label"> 手机号: </label>
76 <input type="text" name="phone" id="phone" datatype="m" errmsg="手机号非法">
77 <span class="Validform_checktip"></span>
78 </div>
79 </t:hasPermission>
80 <div class="form" id="money_id">
81 <label class="Validform_label"> 金额: </label>
82 <input type="text" name="money" id="money" datatype="d" errmsg="金额非法">
83 <span class="Validform_checktip"></span>
84 </div>
85
86 <div class="form">
87 <label class="Validform_label"> 日期: </label>
88 <input type="text" name="date" id="date" class="easyui-datebox">
89 <span class="Validform_checktip"></span>
90 </div>
91
92 <div class="form">
93 <label class="Validform_label"> 时间: </label>
94 <input type="text" name="time" id="time" class="easyui-datetimebox">
95 <span class="Validform_checktip"></span>
96 </div>
97 <div style="text-align:center"><input class="btn" type="submit" value="提交" style="height:30px;width:100px !
98 </div>
99 </fieldset>
100 </t:formvalid>
101 </body>
102 </html>
103 <t:authFilter />
    
```

[2]、页面表单权限配置如下（页面控件编码对应页面控件的 ID）



4.3.2. 手机号字段隐藏 t:hasPermission

表单字段手机号不显示，采用标签<t:hasPermission 来实现，hasPermission 标签比较容易理解，采用包含的方式，对包含的区域根据是否有权限进行动态控制。

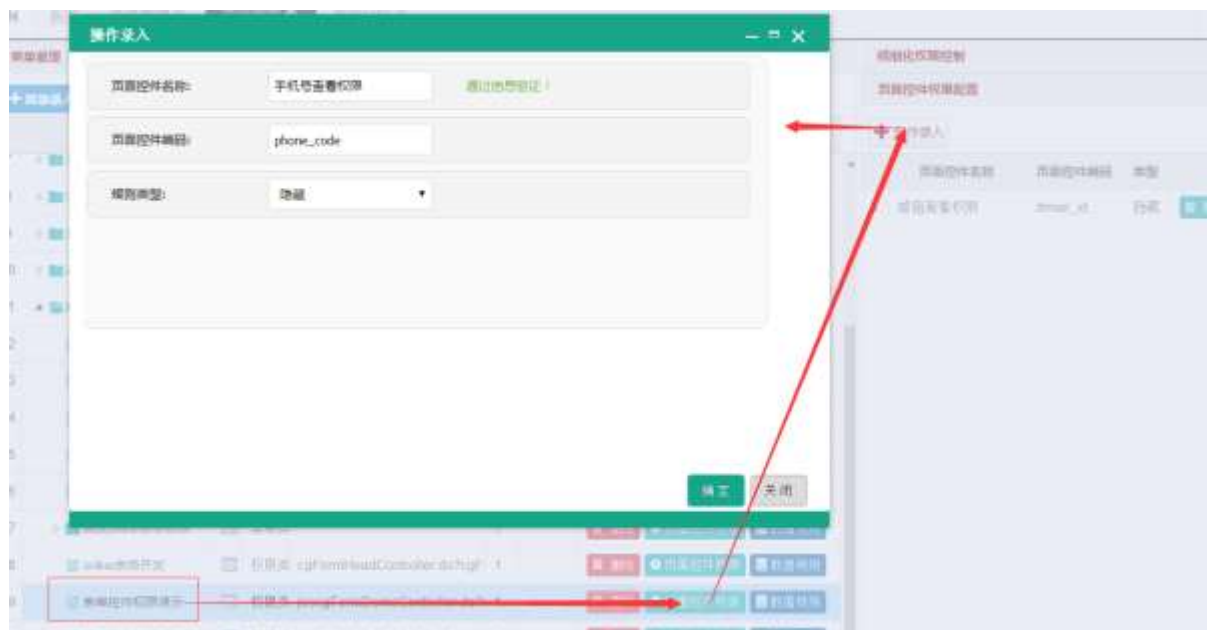
[1]、手机号字段控制隐藏，编码如下

```

62 <input name="shoppingOrder" class="FFZ" id="shoppingOrder" type="checkbox" value="1" /> 加入购物车
63 <span class="Validform_checktip"></span>
64 </div>
65
66
67
68 <div class="form" id="mail_id">
69 <label class="Validform_label"> 邮箱: </label>
70 <input type="text" name="demoorder" id="demoorder" datatype="s" errormsg="邮箱非法">
71 <span class="Validform_checktip"></span>
72 </div>
73
74 <t:hasPermission code="phone_code">
75 <div class="form">
76 <label class="Validform_label"> 手机号: </label>
77 <input type="text" name="phone" id="phone" datatype="s" errormsg="手机号非法">
78 <span class="Validform_checktip"></span>
79 </div>
80 </t:hasPermission>
81 <div class="form">
82 <label class="Validform_label"> 金额: </label>
83 <input type="text" name="money" id="money" datatype="d" errormsg="金额非法">
84 <span class="Validform_checktip"></span>
85 </div>
86
87 <div class="form">
88 <label class="Validform_label"> 日期: </label>
89 <input type="text" name="date" id="date" class="easyui-datebox">
90 <span class="Validform_checktip"></span>
91 </div>
92
93 <div class="form">
94 <label class="Validform_label"> 时间: </label>
95 <input type="text" name="time" id="time" class="easyui-datetimebox">
96 <span class="Validform_checktip"></span>
97 </div>
98 <div style="text-align:center"><input class="btn" type="submit" value="提交" style="height:30px;width:100px !important;" />
99

```

[2]、表单字段权限配置如下



4.3.3. 金额字段禁用 t:authFilter

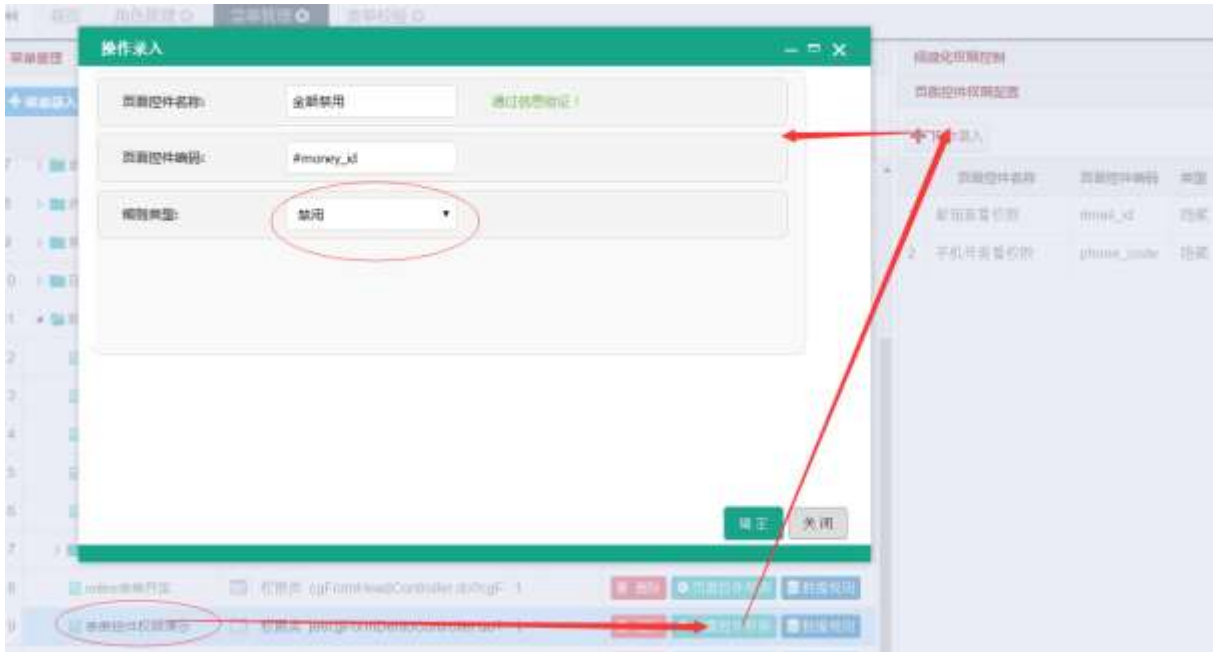
采用标签<t:authFilter />方式。

[1]、通过控件 ID 控制

```

1  form_tag.jsp      form_valid.jsp      HasPermissionTag.java
2  <input name="shoppingfilter" class="PI" id="shoppingfilter" type="checkbox" value="1" /> 添加
3  <span class="Validform_checktip"></span>
4  </div>
5
6
7
8
9  <div class="form" id="mail_id">
10 <label class="Validform_label"> 邮箱: </label>
11 <input type="text" name="demoorder" id="demoorder" datatype="a" errormsg="邮箱非法">
12 <span class="Validform_checktip"></span>
13 </div>
14
15 <t:hasPermission code="phone_code">
16 <div class="form">
17 <label class="Validform_label"> 手机号: </label>
18 <input type="text" name="phone" id="phone" datatype="a" errormsg="手机号码非法">
19 <span class="Validform_checktip"></span>
20 </div>
21 </t:hasPermission>
22 <div class="form" id="money_id">
23 <label class="Validform_label"> 金额: </label>
24 <input type="text" name="money" id="money" datatype="d" errormsg="金额非法">
25 <span class="Validform_checktip"></span>
26 </div>
27
28 <div class="form">
29 <label class="Validform_label"> 日期: </label>
30 <input type="text" name="date" id="date" class="easyui-datebox">
31 <span class="Validform_checktip"></span>
32 </div>
33
34 <div class="form">
35 <label class="Validform_label"> 时间: </label>
36 <input type="text" name="time" id="time" class="easyui-datetimebox">
37 <span class="Validform_checktip"></span>
38 </div>
39 <div style="text-align:center"><input class="btn" type="submit" value="提交" style="height:30px;width:100px;" />
40 </div>
41 </formvalid>
42 </t:formvalid>
43 </body>
44 </html>
45 <t:authFilter />
    
```

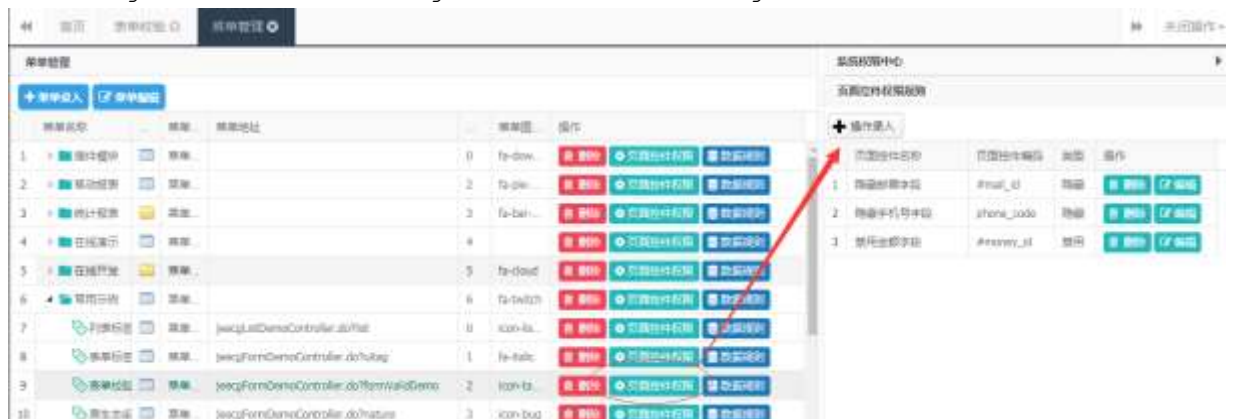
[2]、页面表单字段权限配置如下



4.4. 表单权限配置

针对菜单“ 表单校验”页面请求，`jeecgFormDemoController.do?formValidDemo`，进行表单权限配置。

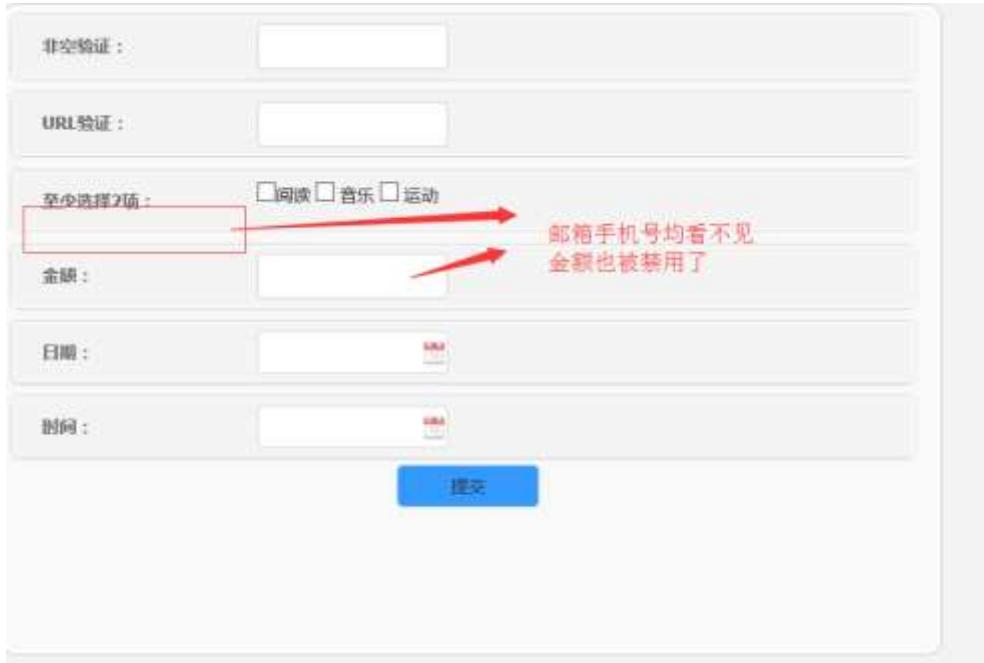
注意：权限请求URL有一定规则要求（目前支持带一个参数，且格式有要求，不能带等号），例如：`loginController.do?login`，不支持等号模式：`loginController.do?name=2`



4.5. 表单权限控制效果

表单权限配置后，未授权用户无法查看字段：[邮箱][手机号]；同时无法编辑[金额] 字段。

采用 demo 用户访问菜单【表单验证】，未授权效果如下：



4.6. 表单权限授权效果

表单权限配置后，默认非授权用户都受控制，只有赋权才解除控制（admin 除外），此时给 demo 角色授权，测试是否看拥有对应的字段操作权限。

[1]、角色授权



[2]、授权效果确认

采用 demo 用户（授权 demo 角色）登录系统效果如下，邮箱字段和手机号字段显示成功，金额字段也可输入。

The screenshot shows a web form with the following elements:

- Navigation: A back arrow and '首页' (Home) link, followed by the active tab '表单校验' (Form Validation).
- Form Fields:
 - '非空验证:' (Non-empty validation) with an empty text input field.
 - 'URL验证:' (URL validation) with an empty text input field.
 - '至少选择2项:' (Select at least 2 items) with three checkboxes: '阅读' (Reading), '音乐' (Music), and '运动' (Sports).
 - '邮箱:' (Email) with an empty text input field and a red error message: '请填写邮箱!' (Please fill in the email!).
 - '手机号:' (Mobile number) with an empty text input field and a red error message: '请填写手机号!' (Please fill in the mobile number!).
 - '金额:' (Amount) with an empty text input field and a red error message: '请填写金额!' (Please fill in the amount!).
 - '日期:' (Date) with a date picker showing '17'.
 - '时间:' (Time) with a time picker showing '16'.
- Submit Button: A blue button labeled '提交' (Submit).

5. 列表数据权限控制

5.1. 功能说明

列表数据权限，主要通过数据权限控制行数据，让不同的角色有不同的访问规则；

比如：销售人员只能看自己的数据；销售经理可以看所有下级销售人员的数据；财务只看金额大于 5000 的数据等等；

5.2. 数据权限控制模式

数据权限控制分两种模式（根据编码风格）

模式一： 列表查询采用 hibernate 方式编码，hibernate 实体，查询采用 Jeecg 的查询过滤器。

实现原理： 数据权限规则，是通过查询过滤器注入的，JEECG 讲数据权限规则以 Hiberate 方式注入到查询条件中；该方式比较简单，不需要额外编码，直接权限配置即可；

模式二： 列表查询采用 minidao 方式(纯 sql)编码，此方式比较复杂需要专题介绍

实现原理： Jeecg 会将数据权限规则，组织成纯 sql 片段，放在 request 线程中，需要开发者，手工编码注入查询逻辑中，**此模式复杂会有专题讲解。**

5.3. 数据权限规则篇

5.3.1. 当前用户上下文变量

注意：数据权限配置，规则值可以填写系统上下文变量（当前登录人信息），从而根据当前登录人信息进行权限控制。

sys_user_code	当前登录用户登录账号
sys_user_name	当前登录用户真实名称
sys_date	当前系统日期
sys_time	当前系统时间
sys_company_code	当前登录用户公司编号
sys_org_code	当前登录用户部门编号

规则值，配置写法如下：`#{sys_user_code}`

5.3.2. 建表规范（系统标准字段）

如果需要通过当前登录人，进行数据权限控制，则业务表必须有以下系统标准字段；数据添加和编辑，jeecg 会通过拦截器自动注入操作人的信息。

比如：创建人，创建时间，创建人所属部门、创建人所属公司，有了这些标准字段，就可以通过当前登录人进行数据隔离控制；

CREATE_BY	系统用户登录账号
CREATE_NAME	系统用户真实名字
SYS_ORG_CODE	登录用户所属部门
SYS_COMPANY_CODE	登录用户所属公司

5.3.3. 组织机构邮编规则

JEECG 组织机构支持无线层级，上下级关系通过组织机构编码实现，组织机构编码规则类似邮编方式，看下图；

邮编规则优势： 邮编规则，上下级编码固定规律，便于定位下级和上级；



5.4. 案例一（行级别 - 限制 demo 用户不能看 admin 的数据）

5.4.1. 数据权限案例

通过权限控制，限制 demo 角色用户，无法查看用户列表中 admin 这条数据。



5.4.2. 数据权限菜单配置

创建数据权限类型菜单（注意：列表访问链接和数据请求链接不是一个，此为加载数据请求）

注意：这里很容易配置错误，一定要注意

用户数据请求地址：userController.do?datagrid

菜单编辑
— □ ×

菜单名称: 菜单名称范围2~15位字符,且不为空

菜单类型:

菜单等级:

父菜单:

菜单地址:

图标:

桌面图标:

菜单顺序:

菜单图标样式: [ace图标样式] [hplus图标样式]

菜单名称	图标	菜单类型	菜单地址	菜单顺序	菜单图标样式	操作
1	自定义菜单	菜单类型		1	自定义图标样式	新增 删除 启用/禁用
2	系统菜单	菜单类型		2	系统图标	新增 删除 启用/禁用
3	用户管理	菜单类型		3	系统图标	新增 删除 启用/禁用
4	系统设置	菜单类型		4	系统图标	新增 删除 启用/禁用
5	系统开发	菜单类型		5	系统图标	新增 删除 启用/禁用
6	系统监控	菜单类型		6	系统图标	新增 删除 启用/禁用
7	运营中心	菜单类型		7	系统图标	新增 删除 启用/禁用
8	系统管理	菜单类型		8	系统图标	新增 删除 启用/禁用
9	系统设置	菜单类型		9	系统图标	新增 删除 启用/禁用
10	系统管理	菜单类型		10	系统图标	新增 删除 启用/禁用
11	数据权限	权限类型	userController.do?datagrid	11	系统图标	新增 删除 启用/禁用
12	用户列表数据权限	权限类型	userController.do?datagrid	12	系统图标	新增 删除 启用/禁用
13	自定义菜单	权限类型	userController.do?datagrid	13	系统图标	新增 删除 启用/禁用
14	自定义菜单	权限类型	userController.do?datagrid	14	系统图标	新增 删除 启用/禁用
15	自定义菜单	权限类型	userController.do?datagrid	15	系统图标	新增 删除 启用/禁用

5.4.3. 数据权限控制规则配置

配置 1、条件规则为非自定义 sql 表达式

操作编辑

规则名称: 用户名 操作名称范围2~20位字符

规则字段: userName

条件规则: 不等于

规则值: admin

确定 关闭

填写说明:

- ① 规则名称: 随意定义
- ② 规则字段: [字段名称]

注意:

模式一: [字段名称]对应着 hibernate 实体的字段

模式二: [字段名称]对应着数据库表的字段

- ③ 条件规则: 大于/大于等于/小于/小于等于/等于/包含/模糊/不等于
- ④ 规则值: 指定值 (固定值/系统上下文变量)

例如:

规则名称: 用户数据限制

规则字段: userName

条件规则: 不等于

规则值: admin

以上表单权限规则表示将动态追加 sql 条件: `userName != 'admin'` 的条件, 即按照用户账号 != admin 进行了数据权限控制。

配置 2、条件规则为自定义 sql 表达式

规则值为自定义 sql 的条件语句

例如如下:

要想筛选年龄小于 18 岁且身高大于 180 的数据即直接配置规则值为：

`age < 18 and height >180`

其中 `age` 和 `height` 均为数据库表字段名



5.4.4. 数据权限授权角色

① 菜单访问授权

用户管理菜单；

② 数据权限授权

用户列表数据数据菜单，数据规则权限授权；



5.4.5. 测试数据权限效果

采用 demo 用户（授权 demo 角色）登录系统，访问用户列表，效果如下，看不到 admin 用户数据，说明权限生效



5.5. 案例二（行级权限 - 登录人只能看自己数据）

5.5.1. 数据权限案例

通过登录人账号，进行数据权限过滤，限制销售人员只能看自己的业务数据。

通过 admin 查看“列表标签”功能如下（数据提前准备，分别采用 demo、scott 两个用户创建）



5.5.2. 数据权限规则配置

控制请求: `jeecgListDemoController.do?datagrid`





5.5.3. 数据权限授权角色

① 菜单访问权限

列表标签菜单;

② 数据权限菜单

Jeecg demo 数据权限列表，数据权限规则授权;



5.5.4. 测试数据权限效果

采用 demo 用户（授权 demo 角色）登录系统，查看菜单【常用实例-列表标签】功能，只能看到自己的数据，说明权限生效。



5.6. 案例三（行级权限 - 登录人可看下级所有人数据）

5.6.1. 数据权限案例

创建三个用户 scott、lisi、demo，设置 demo、scott 为销售人员岗位，设置 lisi 为销售经理属于 demo 和 scott 上级，通过权限配置 lisi 可看下级和自己的业务数据；

采用 admin 用户，查看“列表标签”菜单，可以看所有用户数据



5.6.2. 数据规则配置原理

通过登录人所属部门，进行数据权限配置，查询业务数据通过{创建部门编码}字段，与{当前登录人部门编码}进行模糊匹配；

例如：当前登录人所属部门编码：A01A02

因为 JEECG 设计组织机构编码都是按照邮编方式组织上下级。

销售部门	A01A02	组织机构			删除 查看成员 角色设置
销售经理	A01A02A01	组织机构			删除 查看成员 角色设置
销售人员 销售人员	A01A02A01A01	岗位			删除 查看成员 角色设置

他的下级部门可以用 SQL 这样表示：

`sysOrgCode like 'A01A02%'`

5.6.3. 基础数据准备

① 用户分配组织机构

针对 demo、scott 用户分配销售人员岗位，针对 lisi 用户分配销售经理岗位

	用户账号	用户名称	组织机构	角色	创建时间	状态	
1	demo	demo	销售人员,	demo	2015-05-21	激活	
2	scott	张代浩	销售人员,	普通用户	2016-03-17	激活	
3	lisi	李四	销售经理,	经理角色	2016-03-17	激活	

② 组织机构规则如下，lisi 为 demo、scott 上级。

北京国炬软件		A01	公司					
软件信息部		A01A01	组织机构					
销售部门		A01A02	组织机构					
销售经理		A01A02A01	组织机构					
销售人员	销售人员	A01A02A01A01	岗位					

③ 录入业务数据

使用 scott、demo 两个用户录入数据

查询创建工具 查询编辑器

```
select id,name,age,email,phone,create_by,sys_org_code,sys_company_code from jeecg_demo where create_by in('scott','demo')
```

id	name	age	email	phone	create_by	sys_org_code	sys_company_code
402881875b19f141015b1	测试scott	100	1@qq.com	18611788888	scott	A01A02A01A01	A01
402881875b19f141015b1	测试demo	50	1@163.com	18888888888	demo	A01A02A01A01	A01
402881875b19f141015b1	测试demo部门	1	1@163.com	18677777777	demo	A01A02A01A01	A01
402881875b19f141015b1	测试scott部门	2	1@163.com	18788888888	scott	A01A02A01A01	A01

5.6.4. 数据权限规则配置



说明：通过模糊规则，类似 like ‘{当前登录人组织机构}%'

5.6.5. 数据权限授权角色

设置 lisi 用户为经理角色，对角色分配数据权限



5.6.6. 测试数据权限效果

通过 lisi 用户登录后台，查看“列表标签”功能，发现可以看到 scott、demo 用户录入的数据，说明数据权限生效。



5.7. 案例四（列级别权限 - 不同的人看到数据列表不同的列）

5.7.1. 功能说明

列级别权限，主要针对数据列字段进行权限控制，从而实现不同角色可以有不同列字段查看权限；

5.7.2. 列级别权限案例

通过列数据权限，限制 demo 角色，不能查看列字段[电话]

通过 admin 用户查看“标签列表”功能，界面如下：



5.7.3. 列表页面编码规则

设置标签参数 field，对应页面控制编码；

```
<t:dgCol title="id" field="id" hidden="true" queryMode="group" width="120"></t:dgCol>
<t:dgCol title="名称" field="name" query="true" autocomplete="true" width="120"></t:dgCol>
<t:dgCol title="年龄" extend="{style:'width:50px'}" style="background-color:#3a87ad_50;background-color:#3a87ad_50" field="birthday" formatter="yyyy-MM-dd" queryMode="group" >
<t:dgCol title="部门" field="depId" query="true" queryMode="single" dictionary="t_s_depart,id,depart" >
<t:dgCol title="性别" field="sex" query="true" showMode="radio" dictionary="sex" width="120" extend="{style:'width:50px'}" >
<t:dgCol title="电话" field="phone" queryMode="group" width="120"></t:dgCol>
<t:dgCol title="工资" field="salary" queryMode="group" width="120"></t:dgCol>
<t:dgCol title="创建日期" field="createDate" formatter="yyyy-MM-dd" query="true" queryMode="group" >
<t:dgCol title="邮箱" field="email" hidden="true" queryMode="group" width="120"></t:dgCol>
<t:dgCol title="入职状态" field="status" query="true" extend="{style:{width:'300px';color:'red'}}" >
<t:dgCol title="个人介绍" field="content" hidden="true" queryMode="group" width="500"></t:dgCol>
```

5.7.4. 列表行权限控件配置



```
<t:dgCol title="性别" field="sex" query="true" showMode="radio" dict
<t:dgCol title="电话" field="phone" queryMode="group" width="120"><,
<t:dgCol title="工资" field="salary" queryMode="group" width="120"><
<t:dgCol title="创建日期" field="createDate" formatter="yyyy-MM-dd" q
```

工资查看权限录入同之

5.7.5. 列表行数据权限授权角色



5.7.6. 测试列表行数据权限效果

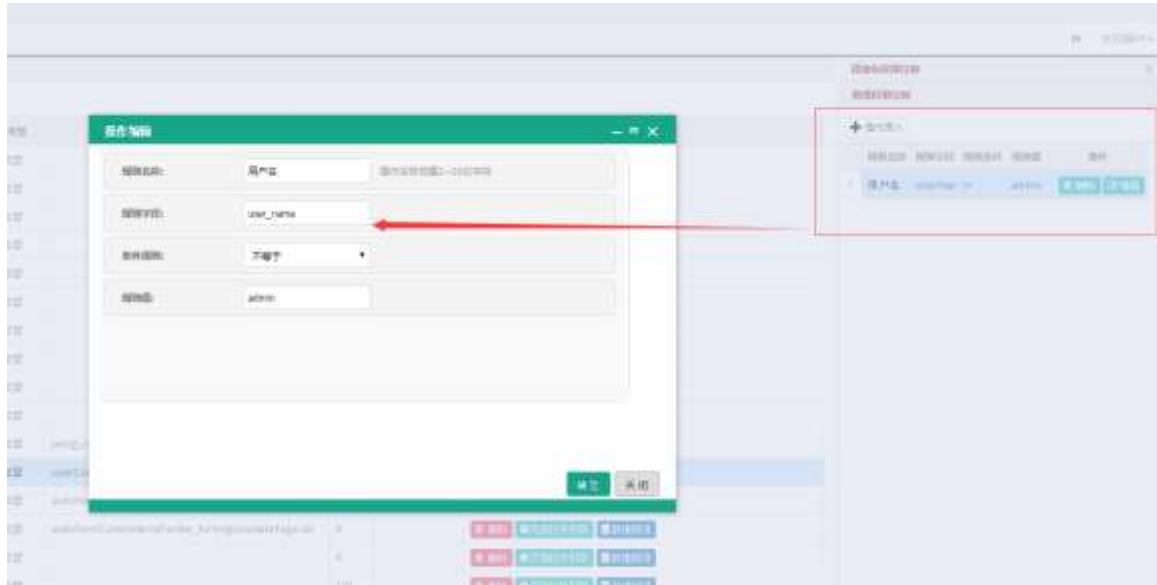
采用 demo 用户（授权 demo 角色）登录系统，访问“标签列表”，效果如下，已经看不到手机号字段，说明列表级权限控制成功。

	名称	年龄	部门	部门code	性别	工资	创建日期	入职状态	操作
1	123xxx	11	北京国炬软件	A01	女性	1.00	2017-04-16	否	查看 删除 刷新
2	小明	12	北京国炬软件	A01	女性	12.00	2017-04-14	否	查看 删除 刷新
3	xiao家	1	北京国炬软件	A01	女性	123.00	2017-04-17	否	查看 删除 刷新
4	22	22	北京国炬软件	A01	女性	1212.00	2017-05-04	否	查看 删除 刷新
5	2222	22	销售部门	A01A02	男性	11.00	2017-05-05	否	查看 删除 刷新
6	qwewqewqew	12	北京国炬软件	A01	女性	12.00	2017-06-05	否	查看 删除 刷新
7	新注册1250	10			女性	0.00	2017-06-28	否	查看 删除 刷新

5.8. 采用 Minidao 方式权限集成

5.8.1. 权限配置规则

说明：SQL 方式数据权限规则一般采用 Minidao 实现数据操作，当然也可以是其他纯 SQL 方式，配置对应数据库表的字段，非实体字段



5.8.1. 权限生成 SQL 规则获取方法

通过工具类 `org.jeecgframework.core.util.JeecgDataAutorUtils`

```

/**
 * 获取请求对应的数据权限规则
 *
 * @param request
 * @return
 */
@SuppressWarnings("unchecked")
public static synchronized List<TSDataRule> loadDataSearchConditonSQL() {
    return (List<TSDataRule>) ContextHolderUtils.getRequest().getAttribute(
        Globals.MENU_DATA_AUTHOR_RULES);
}

/**
 * 获取请求对应的数据权限SQL
 *
 * @param request
 * @return
 */
public static synchronized String loadDataSearchConditonSQLString() {
    return (String) ContextHolderUtils.getRequest().getAttribute(
        Globals.MENU_DATA_AUTHOR_RULE_SQL);
}

```

通过方法：`JeecgDataAutorUtils.loadDataSearchConditonSQLString()`，可以直接获取配置的权限对应的 sql 规则。