|  |
| --- |
| <!-- 设置页面不登录也可以访问的配置 -->  <http pattern=*"/login.html"* security=*"none"*></http>  <http pattern=*"/login\_error.html"* security=*"none"*></http>      <!-- 页面的拦截规则 use-expressions：是否启用SPEL表达式,默认是true-->  <!-- 如果不配置use\_expressions,则access="hasRole('ROLE\_USER')" -->  <http use-expressions=*"false"*>  <!-- 拦截url pattern的/\*：不包括路径下的子目录，只包括根目录当前子目录 /\*\*: 包括项目下的所有目录  access:角色名称，如：ROLE\_USER-->  <!-- 当前用户必须有ROLE\_USER的角色才可以访问根目录及所属子目录的资源 -->  <intercept-url pattern=*"/\*\*"* access=*"ROLE\_USER"*/>    <!-- 开启表单登录功能 -->  <!-- default-target-url默认目标栏 -->  <form-login login-page=*"/login.html"* default-target-url=*"/admin/index.html"* authentication-failure-url=*"/login.html"* always-use-default-target=*"true"*/>  <csrf disabled=*"true"*/>  <!-- 头信息 -->  <headers>  <frame-options policy=*"SAMEORIGIN"*/>  </headers>  <!—登出 -->  <logout/>  </http>    <!-- 认证管理器 -->  <authentication-manager>  <!-- 认证提供者 -->  <authentication-provider>  <user-service>  <!-- 配置当前系统的用户 -->  <!-- authorities：用户属于哪个角色 -->  <user name=*"admin"* password=*"123456"* authorities=*"ROLE\_USER"*/>  </user-service>  </authentication-provider>  </authentication-manager> |

1、如果不设置如下内容，则会提示重定向次数过多

<!-- 设置页面不登录也可以访问的配置 -->

<http pattern=*"/login.html"* security=*"none"*></http>

<http pattern=*"/login\_error.html"* security=*"none"*></http>

2、spring security默认拦截iframe内置框架页，增加如下配置可不拦截：

<headers>

<frame-options policy=*"SAMEORIGIN"*/>

</headers>

3、例如先在地址栏访问localhost:9101/admin/brand.html，然后在登录页输入正确的用户名和密码后，页面直接跳转到brand.html，为了防止跳转页面非index.html的情况，在form-login中添加always-use-default-target=*"true"*

4、<logout/>标签的作用：spring security登出功能。不配置属性的话，则默认跳转到登录页面。

属性：

（1）logout-url: 登出地址

（2）logout-success-url: 登出成功后跳转的地址