Struts中关于用户权限限定的建议 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/214/2021_2022_Struts_E4_B8_AD_E5_c67_214517.htm 关于web系统的权限限定问题，可能有很多的办法，我在这里说一下自己的一些小技巧，起到抛砖引玉的作用，忘各位指正：系统中一个角色包含多个用户，角色和用户之间最好采用一对多，以免发生混乱；自系统初起的时候，系统只有一个超级用户（例如root），有两个默认角色，即游客角色和注册用户角色；超级用户可以在后续管理中添加角色，默认角色不能删除，其他角色的删除中如果这个角色下有用户，可以采取不允许删除或删除后这些用户的角色自动转为注册用户角色；每个角色用户访问系统某些功能模块的权利，某个角色是否可以访问某个功能模块可以由超级用户修改，这里也包括默认角色所对应的权限模块；角色与系统模块之间是多对多的关系，即一个角色可以访问多个模块，一个模块可能有多个角色访问；我们这里主要谈struts，一个模块包含多个action，action和模块是多对一的关系；这样用户访问某个action时会映射到系统的某个模块，这是系统取出当前用户所在的角色，看看这个角色是否有访问此模块的权限，即可以实现struts中的权限设定；这一过程主要包含以下几块：1．系统的各个模块在系统开发完毕后就会形成，这些模块信息保存在持久媒体中；2．struts-config.xml中，每个action的配置中都有一个role属性，这个属性中填写一个模块的名称，这样就建立起了action与模块的多对一关系；3．用户、角色、模块之间的映射关系通过数据库表间的映射，这里就不再多说；4．扩展struts中

的requestProcessor类（注意如果使用tiles框架，需要继承另外一个tiles专用的类），复写其中的processorRole方法（其他方法也很有用，例如preprocess方法，可以设置提交的字符串都为UTF-8，也可以用户写一些系统的访问日志等等），在这个方法中可以取出当前action的模块名称和当前用户的角色，这样就可以实现对于用户的权限限定了。 这样就可以实现权限限定了，这个方法的优点是即便是从某些地方找到下载或者访问某些重要功能的链接仍然可以拦截，缺点是每次访问都需要判定，但做好适当的缓存即可，如何做缓存因各系统而异；如果有特殊需要还可以限定ip，甚至一个session对应一个id，如果换了ip则session立即销毁，防止用户转贴了sessionid所假冒的用户。 