

关键词：软件开发,软件安全策略管理

内容概要：

在软件开发中安全策略管理是非常重要的。网络安全一直都软件在进行软件开发过程中随时都有可能遇到的问题，那么在软件开发中软件安全策略管理应该如何进行才能保证安全？1、安全角色引用。安全角色引用是应用程序提供者用来引用安全角色的标识。应用程序提供...

正文：

在[软件开发](#)中安全策略管理是非常重要的。网络安全一直都软件在进行软件开发过程中随时都有可能遇到的问题，那么在软件开发中[软件安全策略管理](#)应该如何进行才能保证安全？



- 1、安全角色引用。安全角色引用是应用程序提供者用来引用安全角色的标识。应用程序提供者可以用安全角色引用来为安全角色分配资源访问的权限，也可以在安全相关的程序代码中引用安全角色。
- 2、代码授权。J2EE产品通过java 2 安全模型来限制特定J2SE的类和方法的执行，以保护和确保操作系统的安全。
- 3、调用者授权。安全角色：安全角色是具有相同安全属性的逻辑组。它由应用程序的装配者或应用程序的部署者分配的。
- 4、用户和组。用户和组是在实际系统环境下的用户和用户的集合。它们对应着现实当中的人和群体。
- 5、Run As Identities。J2EE 1.3中提供了允许组件开发者和部署者来指定组件以什么身份运行的方法。符合J2EE1.3规范的产品会提供将组件设置成Run As Identities方式的方法。如果Run As Identities方式被选中，在运行中被设置为Run As Identities的组件的调用者不再是调用链中第一个节点的调用者了，而是在部署时被指定的调用者。而调用链中随后节点的调用者也变为与被设置为Run As Identities的组件的调用者相同。
- 6、被传播的调用者身份标识。在J2EE 1.3中可以选择用传播调用者标识作为web组件和ejb组件调用者的标识来进行验证。在这种方式下，整个ejb组件的调用链中interface EJBContext的方法getCallerPrincipal返回相同的主体名。如果调用链中的第一个ejb是被jsp/servlet调用的，interface EJBContext的方法getCallerPrincipal返回的主体名应与interface HttpServletRequest的方法getUserPrincipal的返回值相同。要注意的是在调用链中传递的是用户的标识，而不是凭证，这一点非常重要，因为在调用链的每个节点上用户可能使用不同的安全属性。
- 7、映射。通过映射应用程序的系统管理员将实际系统环境中的用户和角色与安全角色联系起来，从而是实际的用户拥有对企业资源访问的适当授权。
- 8、访问控制。访问控制可以确保安全角色只能访问已授予它安全权限的授权对象。授权对象包括EJB的远程方法、web资源（html

网页, jsp/servlet和多媒体或二进制文件)等。在J2EE中访问控制在应用程序描述文件中与安全角色关联起来。

西安弈聪信息技术有限公司简介

西安弈聪立足陕西西安,为西安企业提供网站优化,软件开发,软件外包,电子政务,网站建设、企业网络营销咨询服务及实施为主体业务,为客户提供一体化IT技术服务。

西安弈聪现有技术架构包含PHP,asp,.NET.C++,VB,J2EE等,在MYSQL,MSSQL数据库系统,ORACLE大型数据库管理系统开发方面专长,经验丰富,是业内技术服务最全面,技术实力最雄厚的IT技术服务企业之一。

联系电话: 029-89322522 4006-626-615 网址:<http://www.xaecong.com> 邮箱:admin@xaecong.com