SpringSecurity简介

安全框架概述

什么是安全框架？ 解决系统安全问题的框架。如果没有安全框架，我们需要手动处理每个资源的访问控制，非常麻烦。使用安全框架，我们可以通过配置的方式实现对资源的访问限制。

常用安全框架

- Spring Security：Spring家族一员。是一个能够为基于Spring的企业应用系统提供声明式的安全访问控制解决方案的安全框架。它提供了一组可以在Spring应用上下文中配置的Bean，充分利用了`Spring IoC`，`DI`（控制反转`Inversion of Control`,`DI:Dependency Injection` 依赖注入）和`AOP`（面向切面编程）功能，为应用系统提供声明式的安全访问控制功能，减少了为企业系统安全控制编写大量重复代码的工作。
- Apache Shiro：一个功能强大且易于使用的Java安全框架,提供了认证,授权,加密,和会话管理。

Spring Security简介

概述

Spring Security是一个高度自定义的安全框架。利用 Spring IoC/DI和AOP功能，为系统提供了声明式安全访问控制功能，减少了为系统安全而编写大量重复代码的工作。使用 Spring Secruity 的原因有很多，但大部分都是发现了 javaEE的 Servlet 规范或 EJB 规范中的安全功能缺乏典型企业应用场景。同时认识到他们在 WAR 或 EAR 级别无法移植。因此如果你更换服务器环境，还有大量工作去重新配置你的应用程序。使用 Spring Security解决了这些问题，也为你提供许多其他有用的、可定制的安全功能。正如你可能知道的两个应用程序的两个主要区域是“认证”和“授权”（或者访问控制）。这两点也是 Spring Security 重要核心功能。“认证”，是建立一个他声明的主体的过程（一个“主体”一般是指用户，设备或一些可以在你的应用程序中执行动作的其他系统），通俗点说就是系统认为用户是否能登录。“授权”指确定一个主体是否允许在你的应用程序执行一个动作的过程。通俗点讲就是系统判断用户是否有权限去做某些事情。

历史

Spring Security 以“The Acegi Secutity System for Spring”的名字始于2003年年底。其前身为 acegi 项目。起因是 Spring 开发者邮件列表中一个问题，有人提问是否考虑提供一个基于 Spring 的安全实现。限制于时间问题，开发出了一个简单的安全实现，但是并没有深入研究。几周后，Spring 社区中其他成员同样询问了安全问题，代码提供给了这些人。2004 年 1 月份已经有 20 人左右使用这个项目。随着更多人的加入，在 2004 年 3 月左右在 sourceforge 中建立了一个项目。在最开始并没有认证模块，所有的认证功能都是依赖容器完成的，而 acegi 则注重授权。但是随着更多人的使用，基于容器的认证就显现出了不足。acegi 中也加入了认证功能。大约 1 年后 acegi 成为 Spring子项目。在 2006 年 5 月发布了 acegi 1.0.0 版本。2007 年底 acegi 更名为Spring Security。