security是什么?

Spring Security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。

security特点有?

提供很多有用的，完全可以指定的其他安全特性。

可能知道，安全包括两个主要操作。

第一个被称为“认证”，是为用户建立一个他所声明的主体。主体一般是指用户，设备或可以在系统中执行动作的其他系统。

第二个叫“授权”，指的是一个用户能否在应用中执行某个操作，在到达授权判断之前，身份的主体已经由身份验证过程建立。

这些概念是通用的，不是Spring Security特有的。

在身份验证层面，Spring Security广泛支持各种身份验证模式，这些验证模型绝大多数都由第三方提供，或者正在开发的有关标准机构提供的，例如 Internet Engineering Task Force.

作为补充，Spring Security 也提供了自己的一套验证功能。

Spring Security 目前支持认证一体化如下认证技术：

HTTP BASIC authentication headers (一个基于IEFT RFC 的标准)

HTTP Digest authentication headers (一个基于IEFT RFC 的标准)

HTTP X.509 client certificate exchange (一个基于IEFT RFC 的标准)

LDAP (一个非常常见的跨平台认证需要做法，特别是在大环境)

Form-based authentication (提供简单用户接口的需求)

OpenID authentication

Computer Associates Siteminder

JA-SIG Central Authentication Service (CAS，这是一个流行的开源单点登录系统)

Transparent authentication context propagation for Remote Method Invocation and HttpInvoker (一个Spring远程调用协议)

Security 有什么作用?

SpringSecurity 是一个安全框架，那它提供了哪些安全措施呢?主要是三个方面，

· 身份认证(你是谁?)

· 权限校验(你能做什么?允许操作的范围)

· 攻击防护(防止伪造身份)

说说Security 流程

1、 首先， 当用户登录时， 前端会把用户输入的用户名、 密码信息传输到后台， 后台用一个类对象将其封装起来，

通常使用的是UsernamePasswordAuthenticationToken这个类。

2、 再来， 到程序负责验证这个类对象。 验证方法是调用Service根据username从数据库中取用户信息到实体类的实例中，

比较两者的密码， 如果密码正确就成功登陆， 同时把包含着用户的用户名、 密码、 所具有的权限等信息的类对象

放到SecurityContextHolder(安全上下文容器， 类似Session) 中去。

3、 其次， 在用户访问一个资源的时候， 需要先判断是否是受限资源。 如果是的话还要判断当前是否未登录，

没有的话就跳到登录页面。

4、 最后!如果用户已经登录， 并访问一个受限资源的时候， 程序要根据url去数据库中取出该资源所对应的

所有可以访问的角色， 然后拿着当前用户的所有角色一一对比， 判断用户是否可以访问。

OAuth2 和JWT区别与联系是?

JWT是一种认证协议

JWT提供了一种用于发布接入令牌(Access Token),并对发布的签名接入令牌进行验证的方法。 令牌(Token)本身包含了一系列声明，应用程序可以根据这些声明限制用户对资源的访问。

OAuth2是一种授权框架

另一方面，OAuth2是一种授权框架，提供了一套详细的授权机制(指导)。用户或应用可以通过公开的或私有的设置，授权第三方应用访问特定资源。