«

Spring / Spring Security

»

Could not find what you were looking for? send us the question and we would be happy to answer your question.

What is Spring Security?

Spring Security provides **comprehensive security services** for Java EE-based enterprise software applications.

There are **two main areas** that Spring Security targets. **"Authentication"** is the process of establishing a principal is who they claim to be (a "principal" generally means a user, device or some other system which can perform an action in your application).**"Authorization"** refers to the process of deciding whether a principal is allowed to perform an action within your application.

What is Oauth?

OAuth is an open standard for authorization. OAuth provides client applications a 'secure delegated access' to server resources on behalf of a resource owner. It specifies a process for resource owners to authorize third-party access to their server resources without sharing their credentials.

What is a security context?

Security context in Spring Security includes details of the principal currently using the application. Security context is always available to methods in the same thread of execution, even if the security context is not explicitly passed around as an argument to those methods.

What is security principal?

SecurityContextHolder stores the principal currently interacting with the application. The principal is the currently logged in user that you retrieve it through the security context.

```
Object principal = SecurityContextHolder.getContext().getAuthentication().getPrincipal();

if (principal instanceof UserDetails) {
String username = ((UserDetails)principal).getUsername();
} else {
String username = principal.toString();
}
```

How do I enable Spring Security in Java Web application?

To enable Spring security in Java Web application, you need to do configure three things,

- declare a delegating proxy filter in web.xml,
- add ContextLoaderListener in web.xml,
- and provide actual security constraints on applicationContext-Security.xml file.

Since Spring security uses a chain of filters to implement various security constraints, also known as security chain filter, it relies on web container for the initialization of delegating filter proxy.

Which filter class is required for spring security?

The DelegatingFilterProxy class from package org.springframework. web.filter is required.

Minimum java and spring version required for spring security?

Spring security 3.0 and jdk 1.5.

Mention other filters in spring security and its purpose.

SecurityContextIntegrationFilter: establishes SecurityContext and maintains between HTTP requests.

LogoutFilter: clears SecurityContextHolder when logout requested.

UsernamePasswordAuthenticationFilter: places Authentication into the SecurityContext on login request.

ExceptionTranslationFilter: converts SpringSecurity exceptions into HTTP response or redirect.

FilterSecurityInterceptor: authorize web requests based on config attributes and authorities.

Types of authentication that spring supports.

- HTTP Basic authentication,
- HTTP digest,
- Form based,
- Using LDAP,
- Using LDAP,
- Using LDAP,
- OAUTH,
- Automatic remember me authentication.

Explain BASIC authentication.

Basic authentication is a simple authentication scheme built into the HTTP protocol. The client sends HTTP requests with the Authorization header that contains the word **Basic** word followed by a space and a **base64-encoded string username:password**.

Explain digest authentication.

Digest authentication is an application of MD5 cryptographic hashing with usage of nonce values to prevent replay attacks. It uses the HTTP protocol.

Does Spring Security support password hashing?

Yes, Spring Security provides support for password hashing.

What is salting in spring security?

Salting secure your application from Dictionary-Attack. Using Salt you may add an extra string in password so hacker find it difficult for braking the password.

There are 2 salt methods,

- Global Salt.
- Per User Salt.

In Global Salt there is one single common word append to password. In Per User Salt we have to give one user attribute serve as Salt String.

How to restrict static resources using spring security?

The Ant matchers match against the request path and not the path of the resource on the filesystem.So ignore any request that starts with "/resources/".This is similar to configuring http@security=none when using the XML namespace configuration.

```
@Override
    public void configure(WebSecurity web) throws Exception {
      web
        .ignoring()
           .antMatchers("/resources/**");
    }
```

Is there a way to set up basic authentication and form login in same application?

Yes. We may need form login for web app and basic for rest services. In that case multiple http configuration is required.

What is JCA in Java?

Java Cryptography Architecture implements security functions for the Java platform. It provides a platform and gives architecture and APIs for encryption and decryption. JCA is used by the developer to combine the application with the security measure. A programmer uses the JCA to meet the security measure. It helps in performing the third party security rules. It uses the hash table, encryption message digest, etc to implement the security.

Custom Search

« JMS »

Comments & Discussions