Spring Security

Course Description

This 2-day course offers hands-on experience with the major features of Spring Security, which includes configuration, authentication, authorization, password handling, testing, protecting against security threats, and the OAuth2 support to secure applications. On completion, participants will have a foundation for securing enterprise and microservices applications.

Course Duration:

2 days

Prerequisites:

Developer experience building applications with Spring Boot, experience using an IDE (Eclipse, Spring Tools, IntelliJ, or VS Code), and experience using build tools such as Maven or Gradle.

Objectives:

By the end of the course, you should be able to meet the following objectives:

- Use Spring Security in Spring and Spring Boot applications
- Configure the Spring Security filter chain
- Protect HTTP endpoints with expression-based access control and the AuthorizationManager API
- Protect method execution
- Use different authentication mechanisms
- Handle passwords in an efficient way
- Integrate Spring Security with Junit 5 and MockMVC to test HTTP and method security
- Protect against common vulnerabilities and threats
- Understand what OAuth2 is
- Use and configure the Spring Authorization Server
- Implement a resource server and client

Course Outline:

1. Security Introduction
   - Need for security
   - Basic security concepts
   - Common security vulnerabilities
2. Spring Security Basics
   - Introduction to Spring Security
   - High-level architecture
   - Overview of SecurityContext
   - Spring Security with Spring Boot
3. Customizing Authentication
   - Building blocks for authentication
   - Authentication mechanisms based on user name and password
   - Other authentication mechanisms
   - Authentication events

4. Securing Web Applications
   - Configuring authorization
   - Using AccessDecisionsManager for authorization
   - Using AuthorizationManager for authorization
   - Bypassing security
5. Method Security
   - Method security architecture
   - Declarative method security with annotations
6. Security Testing
   - Spring Security Testing Support
   - Security mock annotations and meta-annotations
   - Using MockMvc to test security
7. Handling Passwords
   - Password hashing
   - Upgrading passwords
8. (Optional) Protecting Against Common Vulnerabilities
   - Hardening web applications with security headers
   - Preventing cross-site request forgery
   - Encrypting data in transit
9. OAuth2 and OIDC Concepts
   - Need for OAuth
   - Overview of OAuth2 and OIDC
   - OAuth2 grant types
   - Types of tokens
   - Spring Security OAuth2 support and OAuth2 login
10. Spring Authorization Server
    - Introduction to Authorization Server
    - Spring Authorization Server endpoints
    - Spring Authorization Server configuration
11. Protecting and accessing resources with OAuth2
    - Resource server
    - Using JWT tokens
    - Using opaque tokens • Configuring an OAuth2 client

Who Should Attend

Application developers who want to increase their understanding of Spring Security with hands-on experience and build secure Spring and Spring Boot applications.