

# Spring Security

## Course Overview

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 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

## Target Audience

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

## 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.

## Course Delivery Options

- Classroom
- Live Online
- [Private Training](#)

## Course Modules

- 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

## Contact

If you have questions or need help registering for this course, click [here](#).



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 [www.vmware.com](http://www.vmware.com)  
 © 2022 VMware, Inc. All rights reserved. The product or workshop materials is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/download/patents.html>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware warrants that it will perform these workshop services in a reasonable manner using generally accepted industry standards and practices. THE EXPRESS WARRANTY SET FORTH IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE SERVICES AND DELIVERABLES PROVIDED BY VMWARE, OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM. VMWARE WILL NOT BE LIABLE FOR ANY THIRD-PARTY SERVICES OR PRODUCTS IDENTIFIED OR REFERRED TO CUSTOMER. All materials provided in this workshop are copyrighted by VMware ("Workshop Materials"). VMware grants the customer of this workshop a license to use and make reasonable copies of any Workshop Materials strictly for the purpose of facilitating such company's internal understanding, utilization and operation of its licensed VMware product(s). Except as set forth expressly in the sentence above, there is no transfer of any intellectual property rights or any other license granted under the terms of this workshop. If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc., and if outside of the United States, the VMware contracting entity will be VMware International Limited.