

Spring Security and Authentication

Learn how to implement secure authentication and access control in Spring applications.

Category: Programming · Duration: 2 days

WHO IT IS FOR

- Java developers
- Security engineers and system administrators
- Teams that want hands-on practice on real scenarios

In this course, you will gain a comprehensive understanding of Spring Security and learn how to leverage its features to authenticate users and protect your applications from unauthorized access. You will explore various authentication mechanisms, such as username/password, OAuth, and JWT, and discover how to implement role-based access control and secure RESTful APIs. By the end of the course, you will be equipped with the knowledge and skills needed to build robust and secure Spring applications.

Prerequisites

Basic knowledge of Spring Framework and web application development.

Syllabus

- Introduction to Spring Security
- Authentication with username and password
- Authentication with OAuth
- Authentication with JSON Web Tokens (JWT)
- Authorization and access control
- Implementing role-based access control
- Securing RESTful APIs
- Securing web applications
- Using Spring Security with Spring Boot
- Best practices for secure authentication
- Securing third-party integrations
- Securing databases and data storage
- Securing client-side applications

- Implementing single sign-on (SSO)
- Securing microservices architecture
- Monitoring and logging for security
- Testing and debugging security issues
- Securing file uploads and downloads
- Implementing two-factor authentication (2FA)
- Preventing common security vulnerabilities
- Securing session management