Trainings

Web Security Training with Spring Boot

This training focuses on typical requirements for web applications, raises awareness about the most common security risks and imparts practical knowledge on countermeasures in both theory and practice.

Dauer: 2 days

Zielgruppe: Software developers and security engineers (basic knowledge of Spring Boot required)

The Training sessions are usually held in German. Please contact us if you are interested in Training sessions in English.

Increasingly, IT system security is becoming a focal point for companies. This is because they are exposed to potential threats as a result of their networking, architecture and implementations. Many applications are now available online in the form of web apps or APIs, and a single security vulnerability can be enough for attackers to invade the system and cause damage.

To control this risk, security requirements must be considered from the very start of the software development process. Software developers must be aware of attack vectors in order to identify and avoid typical vulnerabilities. This training focuses on typical requirements for web applications, raises awareness about the most common security risks and imparts practical knowledge on countermeasures in both theory and practice.

On the first day of training, participants are sensitised to the risks of inadequate security in web applications. In addition, the most common problem areas are presented using the OWASP Top 10. To make theoretical knowledge hands-on, participants are given the opportunity to hack an intentionally vulnerable web application themselves. After all, only those who know about an attacker’s capabilities can consider and implement appropriate countermeasures when developing a software project.

On the second day, participants will learn how to prevent discovered vulnerabilities already during development. The focus here will be on the Spring Boot platform. Participants learn how Spring Security’s various security mechanisms are structured, how they can be used correctly and which configurations have proved to be successful in practice. Using a sample project, participants can implement this knowledge directly in the code. The training concludes with an outlook on integrating security measures into agile development processes.

Agenda:

Day 1

Motivation: Why is software security important?

- Security as an integral part of modern software systems
- Current threats and requirements

-OWASP Top 10

- The ten most common security risks in web applications
- Countermeasures for defence

Live hacking:

- Independent discovery and exploitation of vulnerabilities in a provided web app that is deliberately vulnerable
- Becoming familiar with the attack capabilities of an attacker

Day 2

Spring Boot security

- Principles, methods and components
- Secure configuration and operation

Practical section: Securing a basic Spring Boot application

- Identification of classic security pitfalls in a Spring Boot context
- Incremental pitfall removal/securing

Security in agile development projects

- Continuous security in the software development lifecycle
- Best practices for methods and activities

Note:

- The course fee includes Training documentation.