Trainings

Web Security Training mit Spring Boot

Dieses Training thematisiert die typischen Anforderungen von Web-Anwendungen, schafft Awareness für die häufigsten Sicherheitsrisiken und vermittelt praktisches Wissen zu Gegenmaßnahmen in Theorie und Praxis.

Dauer: 2 Tage

Zielgruppe: Software-Entwickler:innen und Security Engineers mit Spring-Boot-Grundkenntnissen

Die Sicherheit von IT-Systemen rückt immer mehr in den Fokus von Unternehmen, weil sie durch ihre Vernetzung, Architektur und Implementierung potenziellen Bedrohungen ausgesetzt sind. Eine Vielzahl von Anwendungen ist heutzutage im Internet in Form einer Web-Anwendung oder als API erreichbar und bereits eine einzige Schwachstelle kann genügen, dass Angreifer in das System eindringen und Schaden anrichten können.

Um dieses Risiko beherrschbar zu machen, müssen Sicherheitsanforderungen von Anfang an im Software-Entwicklungsprozess berücksichtigt werden. Dazu müssen sich Software-Entwickler:innen der Angriffsvektoren bewusst sein, um typische Schwachstellen erkennen und vermeiden zu können. Dieses Training thematisiert die typischen Anforderungen von Web-Anwendungen, schafft Awareness für die häufigsten Sicherheitsrisiken und vermittelt praktisches Wissen zu Gegenmaßnahmen in Theorie und Praxis.

Am ersten Trainingstag werden die Teilnehmer:innen für die Risiken mangelhafter Security in Web-Applikationen sensibilisiert. Dazu werden die häufigsten Problemfelder anhand der OWASP Top 10 vorgestellt. Um das theoretische Wissen dann praktisch erlebbar zu machen, bekommen die Teilnehmer:innen die Möglichkeit, eine vorbereitete, absichtlich verwundbare Web-Anwendung selbst zu hacken. Denn nur wenn man die Möglichkeiten eines Angreifers kennt, kann man auch entsprechende Gegenmaßnahmen beim Entwickeln eines Software-Projektes berücksichtigen und implementieren.

Am zweiten Tag lernen die Teilnehmer:innen dann, wie die entdeckten Schwachstellen schon in der Entwicklung verhindert werden können. Dabei wird der Augenmerk auf die Plattform Spring Boot gelegt. Die Teilnehmer:innen erfahren, wie die verschiedenen Sicherheitsmechanismen von Spring Security aufgebaut sind, wie sie korrekt eingesetzt werden und welche Konfigurationen sich in der Praxis bewährt haben. Anhand eines Beispielprojektes können die Teilnehmer:innen dieses Wissen direkt im Code umsetzen. Abgeschlossen wird das Training mit einem Ausblick zur Integration von Security-Maßnahmen in agile Entwicklungsprozesse.

Agenda:

Tag 1 :

- Motivation: Warum ist Software Sicherheit wichtig?
  - Security als integraler Bestandteil moderner Softwaresysteme
  - Aktuelle Bedrohungen und Anforderungen
- OWASP Top 10
  - Die zehn häufigsten Sicherheitsrisiken in Web-Anwendungen
  - Gegenmaßnahmen zur Abwehr
- Live-Hacking:
  - Selbstständiges Finden und Ausnutzen von Schwachstellen in einer bereitgestellten, bewusst verwundbaren Web-App
  - Angriffsmöglichkeiten eines Angreifers kennenlernen

Tag 2:

-

Spring Boot Security
  - Prinzipien, Methoden und Komponenten
  - Sichere Konfiguration und Betrieb

- Praktischer Teil: Absichern einer Spring-Boot-Basisanwendung
  - Identifizieren von klassischen Security-Pitfalls im Spring-Boot-Kontext
  - Inkrementelles Beheben/Absichern der Pitfalls

- Security in agilen Entwicklungsprojekten
  - Continuous Security im Software Development Lifecycle
  - Best Practices für Methoden und Aktivitäten

Hinweis:

- Die Kursgebühr beinhaltet Schulungsunterlagen.