JA100 Sichere Java-Entwicklung

Kurzbeschreibung:

Der Kurs soll Java-Entwicklern einen umfassenden Überblick über typische in Java-Software auftretende Schwachstellen geben, welche Programmierfehler ihnen zugrunde liegen und wie sie von Angreifern ausgenutzt werden. In zwei Tagen werden die wichtigsten Schwachstellenklassen von Web-Anwendungen und Unternehmens-Software unter den folgenden Aspekten besprochen:

- Was ist das zugrundeliegende Problem?
- In welchem Kontext treten die Schwachstellen üblicherweise auf?
- Wie nutzen Angreifer sie aus und wie kann man sie dauerhaft vermeiden?
- Welche Rolle spielen hierbei beliebte Frameworks wie z.B. Spring?

Der Kurs bringt Entwickler auf das gleiche Wissens-Niveau wie die Angreifer und versetzt sie in die Lage, die gängigsten Problem-Muster schnell zu erkennen und zu beheben. Der vermittelte Stoff wird anhand von zahlreichen Real-World-Beispielen veranschaulicht.

Zielgruppe:

Das Web-Seminar **Sichere Java-Entwicklung** ist ideal geeignet für:

- Java-Entwickler

Voraussetzungen:

Die Teilnehmer müssen über Entwicklungserfahrung in Java verfügen. Grundlegende docker-Kenntnisse wären von Vorteil.

Sonstiges:

Dauer: 2 Tage

Preis: 1290 Euro plus Mwst.

Ziele:

Die Teilnehmer lernen das sichere Entwickeln von Java-Anwendungen.

Inhalte/Agenda:

- Einführung
  - Ist Java sicherer als andere Programmiersprachen?
  - Terminologie: Rückkanal, Out-of-Band, Daten-Exfiltration, Reverse Shell
  - Die Bedeutung der Java-Version

- Beispiele für typische Vektoren über HTTP
  - XML External Entity Injection
  - Unsicherer Dateiupload in den verschiedensten Varianten
  - Expression Language und Template Injection, Struts2
  - Die Bedeutung der Java Reflection API

- Gegenmaßnahmen
  - Einschränkung des Rückkanals
  - Funktionierendes Patch-Management
  - Konsequente Eingabeprüfung

- Die Schwergewichte der Java Schwachstellen
  - Unsichere Deserialisierung
  - Deserialisierungs-Gadgets
  - Marshalling-Formate: XML, JSON, AMF und YAML
  - JNDI Injection (insbesondere log4shell)
  - Die Bedeutung verwundbarer Bibliotheken
  - Gegenmaßnahmen
  - JEP290
  - Einschränkung des Rückkanals
  - Funktionierendes Patch-Management

- Weitere Themen
  - Das Problem der RMI Registrys
  - Ungeschützte JMX-Schnittstellen
  - REST-APIs
  - Spring Boot Actuator