# Agenda für Security Seminar, Schwerpunkt Web-Anwendungen und Web Services für DAVASO Holding GmbH

Dr. Rainer Sawitzki, 18.6.2020

**Terminvorschlag:** 13.-14.7.2020 oder bevorzugt 23.-24.7.2020

**Ort:** Beim Kunden in Leipzig

**Zielgruppe:** Entwickler

**Vorkenntnisse:** Kenntnisse der Entwicklung von Web-Anwendungen und RESTful WebServices mit Spring Boot.

**Methode:**

- Vortrag, Präsentation, Diskussion, Übungen
- Übungsanteil etwa 30%.

**Technische Voraussetzungen:**

- Jeder Teilnehmer hat eine eigene Umgebung mit
  - Java-Installation (>= Java 8)
  - Entwicklungsumgebung Eclipse in einer einigermaßen aktuellen Version
  - Web Browser mit Debug-Tools, bevorzugt Firefox
  - Internet-Zugang
  - Freier Download von Java-Bibliotheken entweder über das Internet oder über ein internes Artefakt-Repository. Hier ist zu garantieren, dass die Entwickler korrekte Einstellungen (Proxy, Credentials) getroffen haben.
  - Docker-Installation entweder unter Windows 10 oder Linux. Auch hier muss der Download von Images direkt von Dockerhub oder einem internen Repository-Server gewährleistet sein.
- Der Referent benötigt für seine Präsentation
  - Seminarraumausstattung mit Flipchart + Papier, 4farbigem Stiftsatz (möglichst neu) und Projektor mit HDMI-Anschluss.
  - Internet-Zugang über WLAN oder LAN. Ein Zugriff auf das interne Netzwerk ist nicht notwendig.

**Dauer:**

- 2 Tage mit jeweils 4 Unterrichtseinheiten mit jeweils 90 Minuten, 6 Stunden netto Seminarzeit pro Tag.
- Vorschlag für die Seminarzeiten: 9:00 - 16:15 mit zwei Kaffeepausen 15’ sowie Mittagspause 45’ 12:15-13:00.

**Ausgangssituation:**

- Der Kunde betreibt verschiedene Web-Anwendungen auf Java-Stacks (Klassische Web-Anwendung mit JSF/Spring Core bzw. eine REST-Architektur mit Spring Boot/Thymyeleaf), die jeweils mit Hilfe von Spring Security abgesichert sind.
- Identity&Access Management wird in einem Keycloak-Server realisiert.

**Inhalte**, in Klammern jeweils die geschätzte Anzahl von Unterrichtsblöcken)**:**

- Von Injection zu CORS: Typische Angriffsvektoren für Web-Anwendungen am Beispiel der OWASP-Top 10 (1)
- Einführung in die Architektur und Arbeitsweise von Spring Security (1)
- Grundlagen von Keycloak mit OpenID Connext und JWT (1)
- Eine Spring Boot-Anwendung mit Anbindung an Keycloak über Spring Security, Übertragen der Kenntnisse auf eine JSF-Anwendung (2)
- Integration von Security-Themen in (automatisierte) Tests: Security Audits, Smoke und Penetration-Tests, ....(2)
- Diskussion/Review der bisherigen Umsetzungen beim Kunden, Fragerunde, Feedback (1)