



---

# Sicherheit in Webanwendungen Erweitert

Dauer: 2-4 Tage

## Beschreibung:

Im Rahmen dieser Schulung lernen Web-Entwickler die häufigsten Bedrohungen für Webanwendungen kennen und welche Gegenmaßnahmen getroffen werden können. Als Beispiel-Anwendung mit absichtlich bestückten Schwachstellen dient das OpenSource Projekt Juice Shop.



Die erlernten Konzepten lassen sich auf jede Programmiersprache und Architektur anwenden.

Für das liebevolle Wohl der Teilnehmer während der Schulung von sorgfältig ausgewählten Lieferanten ist gesorgt.

Die Teilnehmer kennen nach Abschluss des Moduls die Bedeutung der Web-Sicherheit für Unternehmen und Organisationen. Sie eignen sich theoretisches Grundlagenwissen und darauf aufbauendes Methodenwissen an, um eine (einfache) Risiko-Bewertung von Web-Anwendungen durchzuführen sowie Ansätze zur Absicherung anbieten zu können. Sie erlangen Verständnis des Zusammenspiels zwischen dem Software-Entwicklungsprozess und Sicherheit.

## Inhalt:

- Kurzer Einstieg in Web-Grundlagen
- Grundlagen der IT-Sicherheit
- Web-Risiken orientiert an den OWASP Top Ten 2017
- Übungen bestehen aus einem Angriffs-Teil, bei welchem zunächst die Bedrohung durch praktisches ausprobieren erlernt wird und aus einem Abwehr-Teil, bei dem Maßnahmen zur Minderung oder Abwehr der Bedrohung vorgestellt oder Implementiert werden
- Sicherheit im Entwicklungszyklus
- Docker-Sicherheit für Entwickler
- Mobile Sicherheit
- In den letzten drei Stunden stellen die Teilnehmer im Rahmen eines Capture the Flags ihr erworbenes Wissen unter Beweis



**Zielgruppe:**

Alle Personen die mindestens seit zwei Jahre in der Entwicklung von Webanwendungen tätig sind und bei denen Folgendes keine Fragezeichen auslöst: HTML, HTTP, SQL, noSQL, Datenbank, Browser, <script> und API.

