

iSAQB Advanced Web Security

Ziel und Nutzen

Das erlernte Wissen lässt sich sowohl in Architektur als auch Entwicklung unabhängig von Technologien und Sprachen einsetzen.

Schreibe sichere Webanwendungen ohne externe Spezialist:innen.

Es ermöglicht dir, Verantwortung für die Sicherheit deiner Software-Architektur zu übernehmen.

Zielpublikum

Software-Architekt:innen und -Entwickler:innen profitieren zu jedem Zeitpunkt im Entwicklungszyklus vom erlernten Wissen. Denn Security berührt jede Ebene von Entwurf, Entwicklung, Test und Betrieb: Wenn ein Software-Produkt erst nach Abschluss der Entwicklung »sicher« gemacht werden soll, ist es meist schon zu spät.

Inhalt

Dieser Kurs wird durchgeführt von Socreatory

Der Betrieb eines Softwaresystems geht immer mit dem Risiko eines Angriffs einher. Sei es durch Ausnutzung von Schwachstellen in verwendeten Bibliotheken, eigene Nachlässigkeiten oder Social Engineering. Insbesondere weltweit erreichbare Webanwendungen sind einer Vielzahl von Angriffen ausgesetzt.

Das Advanced-Modul WEBSEC versetzt dich in die Lage, typische Angriffsmethoden zu erkennen, Risiken bei der Entwicklung von Webanwendungen zu bewerten und durch eine saubere Architektur und klare Kommunikation zu unterbinden.

- Risikoanalyse
- Security-Gates, Review und
- Kryptographie
- Authentifizierungsarten & Autorisierungskonzepte
- Gefahren von Social Engineering & Man-in-the-Middle-Angriffen
- Intrusion Detection, Einsatz von TLS
- Sicherer Entwurf- und Entwicklungsprozess
- Incident Management
- Technische Grundlagen für die sichere Webentwicklung
- Bekannte Angriffe und Angriffsvektoren im Web
- Security und Infrastruktur im Web

Voraussetzungen

iSAQB Foundation