

IT-SICHERHEIT

Lernziele

Ziel des Moduls ist es, die Teilnehmenden in die Lage zu versetzen, die „Industry Best Practices“ im Bereich der sicheren Software-Entwicklung auf Software anzuwenden. Dies umfasst sowohl analytische („Penetration Testing“) als auch konstruktive („Secure SDL“) Vorgehensweisen.

Lehrinhalte

1. Grundsätze der sicheren Software-Entwicklung, Vorgehensmodelle und Prozesse, einschlägige Normen und Standards
2. Sicherheitsanforderungen und Akzeptanzkriterien, speziell für nicht-funktionale Sicherheitsanforderungen
3. Sicheres Design und Bedrohungsmodellierung, Architekturanalysen, Security Design Patterns
4. Wichtige Security Design Patterns, Architekturgrundlagen und Sicherheitskonzepte, wie etwa:
 - Identitäts- und Berechtigungsmanagement
 - Förderationskonzepte
 - Sichere Web-Services
 - Kryptographische Primitive und Protokolle
 - Einsatz von Vertrauensgrenzen und „defense in depth“
6. Grundlagen der sicheren Programmierung, Sicherheitstests, Penetrationstests, Tools zum Testen
7. Sichere Einrichtung und sicherer Betrieb
8. Security Response: Umgang mit Schwachstellen, die durch andere entdeckt werden

Dauer	4-6 Wochen
Ort	Hochschule Aalen
Niveau/Level	Master
Voraussetzungen	Formal: Keine Inhaltlich: Bisherige Projektergebnisse aus anderen Modulen, die für eine Security-Überarbeitung / -Ergänzung herangezogen werden können.
Sprache	DE

Workload	20 UE Präsenz 30 UE geleitetes E-Learning 100 UE Selbststudium/Prüfungsvorbereitung
Didaktisches Konzept	Dies ist ein Blended Learning Modul, bei dem sich Online- und Präsenzunterricht abwechseln.
Prüfungsform	Portfolio
Abschluss	Hochschulzertifikat mit ECTS nach bestandener Prüfung
Kursgebühr	1.600 EUR
Fördermöglichkeit	ESF

