

Security for Web- and Mobile Applications

Ziel und Nutzen

Das Seminar soll dem Teilnehmer ermöglichen, mehr Hands-On Erfahrung im Bereich Web und Mobile Security zu sammeln. Die im Kurs verwendete Laborumgebung erlaubt den Kursteilnehmern dieses Wissen anzuwenden und praktische Erfahrung zu sammeln. Insbesondere soll dieses Wissen bei der täglichen Arbeit im Bereich Prävention, Antizipation und Reaktion auf Cyber-Attacken unterstützend wirken.

Zielpublikum

Software Entwickler im Web oder Mobile Umfeld.

Inhalt

Das Training zum Thema Web und Mobile Security beinhaltet sowohl die Vermittlung der Theorie als auch das Bearbeiten von Laborübungen. Es werden also typische Bedrohungs-, Angriffs- und Fehlerszenarien für Webanwendungen, Webservices und Mobile Apps behandelt. Das Training hat zum Ziel, den Teilnehmenden Wissen an die Hand zu geben, um die Vertraulichkeit, Integrität und Verfügbarkeit ihrer eigenen Systeme und Anwendungen garantieren zu können.

Die Schulung beinhaltet folgende Themen:

- OWASP Top 10
- Injections (SQL, LDAP, XML, usw.)
- Authentication bypasses, Authorization und Access Control issues
- Session Handling issues
- Same Origin Policy
- Cross Site Scripting
- Cross-origin Ressource Sharing
- Content Security Policy, Subresource Integrity
- NodeJS Spezifikas
- AngularJS Spezifikas
- Webservice Security
- SAML 2
- Misconfigurations
- Kanalverschlüsselung
- Web Application Firewall
- Security Architektur Android und iOS
- Netzwerk Analyse, Man in the Middle
- SSL/TLS Trust mit erweiterter Validierung

Voraussetzungen

Kenntnisse in Web Technologien