Sicherheit für Webentwickler

Workshop Ziele

In diesem intensiven 3-Tages-Workshop erlangen Sie ein umfassendes Verständnis für die grundlegenden und fortgeschrittenen Aspekte der IT-Sicherheit mit speziellem Fokus auf Webentwicklung.

Sie lernen praxisnah, wie Sie Sicherheitslücken identifizieren, Angriffe abwehren und sichere Webanwendungen entwickeln können. Anhand der OWASP Top 10 und weiterer relevanter Themen erwerben Sie Fähigkeiten, die Sie direkt in Ihrem Arbeitsalltag anwenden können.

Tag 1: Einführung in die Web-Sicherheit und OWASP Top 10

Begrüßung und Einführung

- Vorstellung des Trainers und der Teilnehmer
- Überblick über die Workshop-Ziele und den Ablauf

Einführung in die IT-Sicherheit

- Bedeutung der Sicherheit in der Webentwicklung
- Aktuelle Bedrohungslage und typische Angreifer

Praktische Übungen im Labor

- Einrichtung der Laborumgebung
- Einfache Übungen zu jeder OWASP Top 10 Schwachstelle
- Identifikation und Ausnutzung von Sicherheitslücken
- Diskussion von Gegenmaßnahmen und Best Practices

OWASP Top 10 Sicherheitsrisiken

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfigurations
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Verwendung von Komponenten mit bekannten Schwachstellen
- Unzureichendes Logging und Monitoring

Tag 2: Automatisierte Sicherheitstests mit Tools

Einführung in automatische Sicherheitstools

- Vorteile und Grenzen automatisierter Tests
- Überblick über gängige Tools

Arbeit mit SQLMap

- Funktionsweise von SQLMap
- Erkennung von SQL-Injection-Schwachstellen
- Durchführung von Scans auf Test-Webanwendungen
- Analyse der Ergebnisse und Behebung von Schwachstellen

Einsatz von Metasploit

- Einführung in das Metasploit Framework
- Module und Exploits verstehen
- Anwendung von Metasploit auf bekannte Schwachstellen
- Absicherung gegen die identifizierten Angriffe

Verwendung von CMS-Sicherheitsscannern

- Sicherheitsrisiken in Content-Management-Systemen (CMS)
- Vorstellung von Tools wie WPScan, Droopescan, CMSmap usw.
- Scannen von CMS wie WordPress, Drupal, Typo3 und anderen
- Identifikation von Plugins, Themes oder Modulen mit Sicherheitslücken
- Umsetzung von Sicherheitsmaßnahmen und Updates

Weitere nützliche Tools

- Burp Suite
- Nikto
- Nmap für Webentwickler

Tag 3: Praktische Übungen in realitätsnaher Umgebung

Praktische Anwendung des Gelernten

- Arbeiten in einer simulierten Kundeninfrastruktur
- Durchführung eines vollständigen Sicherheitstests einer Webanwendung

Szenario-basierte Übungen

- Identifikation und Ausnutzung von Schwachstellen in komplexen Umgebungen
- Priorisierung der gefundenen Sicherheitslücken nach Relevanz
- Anwendung der Tools und Techniken aus Tag 1 und 2
- Dokumentation der Ergebnisse und Erstellung eines Berichts

Best Practices und Abschluss

- Sichere Programmierstandards und -richtlinien
- Einsatz von Security-Frameworks und -Bibliotheken
- Integration von Sicherheitsüberprüfungen in den Entwicklungsprozess
- Zusammenfassung und Wiederholung der wichtigsten Lerninhalte
- Austausch von Erfahrungen und Erkenntnissen

Ihr Trainer: Sebastian Schlaak

Aus der Anwendungsentwicklung kommend, habe ich mich in den letzten Jahren auf Künstliche Intelligenz und IT-Sicherheit spezialisiert. Mit einem Master in Informatik, einem Master in Management und einem Leadership-Zertifikat von der Stanford Graduate School of Business vereine ich technisches Know-how mit betriebswirtschaftlichem Verständnis.

Meine Rollen als Senior Developer, CTO und Geschäftsführer in verschiedenen Unternehmen haben mir tiefe Einblicke in die Herausforderungen moderner Unternehmen gegeben und ermöglichen es mir, hands-on Lösungen zu bieten.