Einführung in die Web-Sicherheit

Sicherheitskonzepte, Angriffe und Gegenmassnahmen für Webanwendungen – unabhängig vom Framework, mit praktischen Übungen.

2 TAGE | FORTGESCHRITTEN | REMOTE ODER INHOUSE | DEUTSCH & ENGLISCH | BIS ZU 12 TEILNEHMENDE (MEHR AUF ANFRAGE)

FÜR WEN

- Web-Entwicklerinnen und -Entwickler aller Frameworks
- Teams, die Security-Anforderungen aus Audits umsetzen müssen
- Tech Leads, die Sicherheitsentscheidungen treffen

DANACH KANN EUER TEAM

- Die wichtigsten Angriffe auf Webanwendungen erkennen und einordnen
- Sicherheitskonzepte wie Same-Origin-Policy, CORS und CSP korrekt einsetzen
- Eine Webanwendung selbst auf Schwachstellen prüfen

VORAUSSETZUNGEN

- Kenntnisse in HTML, CSS, JavaScript und HTTP
- Keine Security-Vorkenntnisse nötig
- Laptop mit Browser und Editor

Ein framework- und sprachunabhängiger 2-Tages-Workshop zu Web Security: von den Grundlagen der IT-Sicherheit über Sicherheitskonzepte wie CORS, CSP und OAuth bis zu Angriffen aus den OWASP Top 10 und deren Abwehr – mit praktischen Übungen.

Ihr arbeitet mit Angular und wollt direkt die Angular-spezifischen Themen wie Trusted Types, CSP für Angular und Tokens im Frontend? Dann passt der Kurs **Angular Security** besser.

AGENDA

Reihenfolge und Tiefe der Blöcke passen wir an euer Team an – was ihr schon beherrscht, lassen wir weg, eure Fragen bekommen die Zeit.

01 IT-Security-Grundlagen

- CIA-Triade / Sicherheitsprinzipien
- Verschlüsselung
- Hashing
- Symmetrische / asymmetrische Verschlüsselung
- Authentication & Authorization

02 Sicherheitskonzepte in Webanwendungen

- Same-Origin-Policy / Cross-Origin Resource Sharing (CORS)
- Cookie-Sicherheit (Cookie-Attribute wie httpOnly)
- HTTP-Sicherheit
- Richtiger Einsatz sicherheitsrelevanter HTTP-Header
- Content Security Policy (CSP)
- JWT
- OAuth2 und OpenID Connect
- uvm.

03 Praktische Anwendung der Sicherheitskonzepte

- Wie man Datenintegrität sicherstellt, selbst wenn diese
  - über unsichere Kanäle laufen
  - den Kommunikationsweg absichert
  - Anwendungen mehrstufig schützt

04 Angriffe auf Webanwendungen

- OWASP Top 10
- Credential Attacks
- Cross-Site-Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Diverse Injection-Attacken (z. B. SQL)
- DoS

        - Passwörter sicher speichert und
    - Worauf man achten muss bei einer
        - Authentifizierungs-Implementierung
        - Einsatz eines Web-Frameworks
    - Sichere Implementierung von
        - Formularen und Datei-Uploads
        - Denial-of-Service-Absicherungsstrategien
        - Sicherheitsmassnahmen für das Frontend und
        - Sichere API-Entwicklung u.a. mit REST-Services

05 Absicherung von Webanwendungen

- Gegenmassnahmen zu allen vorgestellten Angriffsvektoren

06 Einführung in das Prüfen auf Schwachstellen einer Webanwendung

- Manuelle und automatische Werkzeuge
- Statische und dynamische Analyse zum Scannen auf Sicherheitslücken

EUER TRAINER



Martina Kraus

GOOGLE DEVELOPER EXPERT

Application Security Engineer und Google Developer Expert, spricht auf internationalen Konferenzen über Web-Sicherheit und organisiert die NG-DE mit.

TRAINING ANFRAGEN

- Nur für euer Team – Remote oder Inhouse
- bis zu 12 Teilnehmende (mehr auf Anfrage)
- ab CHF 2’400 pro Tag für das ganze Team
- Vor Ort: zuzüglich Reisekosten
- Fixes Angebot innerhalb eines Werktags
- Das Erstgespräch ist kostenlos und unverbindlich
- Deutsch oder Englisch
- Sitz bei Zürich – vor Ort in CH, DE, AT; remote überall

Training anfragen: offering.solutions/de/training-introduction-to-web-security/ · mail@offering.solutions