Einführung in die Web-Sicherheit

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

2 DAYS | INTERMEDIATE | REMOTE OR IN-HOUSE | GERMAN & ENGLISH | UP TO 12 PARTICIPANTS (MORE ON REQUEST)

WHO IT'S FOR

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

AFTERWARDS YOUR TEAM CAN

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

PREREQUISITES

- 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

The order and the depth of each block are adapted to your team – topics you already master are skipped, your questions get the time instead.

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

YOUR TRAINER



Martina Kraus

GOOGLE DEVELOPER EXPERT

Application Security Engineer and Google Developer Expert, speaks about web security at international conferences and co-organizes NG-DE.

REQUEST A TRAINING

- For your team only – Remote or in-house
- up to 12 participants (more on request)
- from CHF 2,400 per day for the whole team
- On site: plus travel at cost
- Fixed quote within one business day
- The first call is free and without obligation
- German or English
- Based near Zurich – on site in CH, DE, AT; remote everywhere

Request this training: offering.solutions/training-introduction-to-web-security/ · mail@offering.solutions