Angular Security

XSS, CSP, Trusted Types, OAuth und OIDC – was eine Angular-Anwendung wirklich schützt und wie euer Team es umsetzt.

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

FÜR WEN

- Angular-Entwicklerinnen und -Entwickler
- Teams mit Anwendungen, die Logins, Tokens oder sensible Daten verarbeiten
- Teams, die ein Security-Audit vorbereiten

DANACH KANN EUER TEAM

- XSS in Angular verhindern und Trusted Types einsetzen
- Eine Content Security Policy für die eigene App aufsetzen
- Tokens im Browser sicher handhaben und OAuth 2.x/OIDC korrekt integrieren
- Die eigene Anwendung auf Schwachstellen prüfen

VORAUSSETZUNGEN

- Praktische Angular-Erfahrung
- Grundwissen zu HTTP und Browser-Sicherheit hilft, ist aber nicht nötig
- Laptop mit eurer üblichen Entwicklungsumgebung

Angular schützt von sich aus vor vielen Angriffen – aber nicht vor allen, und nicht, wenn man es falsch einsetzt. In zwei Tagen lernt euer Team die Grundlagen der Browser-Sicherheit, XSS-Abwehr mit Trusted Types, eine Content Security Policy für Angular und den sicheren Umgang mit Tokens, OAuth 2.x und OIDC – mit der eigenen Anwendung als Beispiel.

Ihr braucht zuerst die framework-unabhängigen Grundlagen, oder euer Team arbeitet nicht mit Angular? Dann startet mit der **Einführung in die Web-Sicherheit**.

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 Grundlagen der Browser-Sicherheit
- Same-Origin-Policy und Cross-Origin Resource Sharing (CORS)
- Konfigurieren von Browser-Sicherheitsmechanismen
- Umgang mit bösartigem JavaScript

02 Einführung in Cross-Site Scripting (XSS)
- XSS-Abwehr in Angular / DomSanitizer
- XSS-Fallen in Angular
- Verwendung von Trusted Types mit Angular

03 Einsatz der Content Security Policy (CSP)
- Einführung in die CSP
- Häufige Sicherheitsfehler in CSP-Richtlinien
- CSP für Angular bereitstellen
- CSP in der Praxis
- Sichere Frontend-Architekturen

04 Sandboxing nicht vertrauenswürdiger Inhalte
- Architekturelle Sicherheitsmuster
- Sicherung von Tokens im Browser
- Erweiterte OAuth-2.0/2.1-Sicherheit

05 Häufige OAuth 2.x und OIDC-Bereitstellungsmuster

06 Einführung in das Prüfen auf Schwachstellen einer Webanwendung
- Manuelle und automatische Werkzeuge

- Sicherheitsbegrenzungen von OAuth 2.x in Frontends
- Sicherung von Frontends mit einem Backend for Frontend (BFF)
- Sicherheitsempfehlungen für die Verwendung von OAuth 2.x in Angular
- 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-angular-security/** · mail@offering.solutions