Orientation in Objects

⟩ Seminar ⟩

REST und API Sicherheit

REST APIs basieren auf Web-Technologien, unterscheiden sich aber von Web Anwendungen und weisen andere Bedrohungspotentiale sowie Risiken auf. Die Besonderheiten bei der Absicherung von APIs bilden den Schwerpunkt dieser Schulung. Die Grundlagen werden im Kurs mit anschaulichen Beispielen, Übungen und Demonstrationen behandelt.

Seminar-Inhalt

Angriffsvektoren bei REST APIs
- Die OWASP Top 10 Risken
- SQL-, XML- und Skript-Injection Angriffe
- CSRF, DoS und Man in the Middle Attacken

Grundlagen der Sicherheit und Kryptographie
- Verfügbarkeit, Vertraulichkeit, Integrität
- Authentifizierung, Authorisierung und Nichtabstreitbarkeit
- Grundbegriffe: Identität, Token, Hashalgorithmus, ...
- Digitaler Fingerabdruck, Hashfunktion & Digest
- Sicherheit von Hash Algorithmen
- Symmetrische Verschlüsselung mit dem AES Algorithmus
- Asymmetrische Verschlüsselung

Kryptographie mit öffentlichen Schlüsseln
- X.509 Zertifikate und digitale Signaturen
- Das Root-Zertifikat
- Signieren von URLs und Anfragen

SSL
- Verschlüsselung und Authentifizierung
- Basic Authentication mit SSL
- Server- u. Client Zertifikate
- Welche TLS Versionen sind sicher?

API Gateways
- API Gateway als Firewall
- Granularität der Zugriffsrechte

SSO für APIs
- OAuth, JWT oder SAML?
- Integration mit LDAP
- Weiterreichen der Identität des Aufrufers an Downstream Services

API Schlüssel
- Vorteile von API Keys gegenüber Passwörtern
- Ausgabe von API Schlüsseln über Portale
- Sichern eines "Public APIs" mit Keys

OAuth
- Ablauf einer OAuth2 Autorisierung
- Implementierungen: Spring Security OAuth
- OAuth2 im Social Web und im Unternehmen

OpenID Connect
- Ablauf einer Authentifizierung
- ID Tokens
- Produkte

JSON Web Token und Web Encryption
- Single Sign On SSO mit JWT
- Aufbau eines JWT Token
- Signieren von JWT Tokens

Eingabe-Validierung
- Wie man SQL-, XML- und Code-Injection verhindern kann
- Check von Query- und Path-Parametern
- White- und Blacklists
- HTML Sanitizer, Input Sanitization, Escaping

API Gateways
- Funktionsweise eines Reverse Proxy
- Rate Limiting und Quotas
- Cross-Origin Resource Sharing CORS erleichtern

Zielgruppe

Entwickler, Sicherheitsbeauftragte und Projektmanager

Voraussetzungen für Seminar-Teilnahme

IT Grundlagen

Seminar-Dauer

2 Tage

Vorteile einer Seminar-Teilnahme

- Erlernen Sie die theoretischen Grundlagen zur Absicherung Ihrer Schnittstellen
- Verschaffen Sie sich einen Überblick über mögliche Angriffsszenarien und lernen Sie geeignete Gegenmaßnahmen kennen
- Unsere Kurs-Unterlagen sind immer auf dem aktuellsten Stand

Seminar-Preis

1.460 EUR pro Person
(inkl. Unterlagen u. Tagesverpflegung zzgl. MwSt.)

Seminar-Termine

21.6. - 22.6.2018, 29.11. - 30.11.2018 (Bonn)

Inhouse-Kurse

Alle unsere Seminare können wir Ihnen auch für eine Durchführung in Ihrem Hause mit einer speziellen Kalkulation für Exklusiv-Seminare anbieten. Hierbei können die Inhalte aller unserer Seminare beliebig für Ihr individuelles Training zu einem Wunschseminar zusammengestellt werden.