

API security in Node.js (ASINJS)

ID ASINJS Preis auf Anfrage Dauer 3 Tage

Zielgruppe

API-Entwickler in JS und TS

Voraussetzungen

Allgemeine JS/TS-Entwicklung

Kursziele

- Vertrautmachen mit grundlegenden Konzepten der Cybersicherheit
- · Verständnis von API-Sicherheitsfragen
- Detaillierte Analyse der OWASP API Security Top Ten Elemente
- Einordnung der API-Sicherheit in den Kontext von JS/TS
- Über die niedrig hängenden Früchte hinausgehen
- Verwaltung von Schwachstellen in Komponenten von Drittanbietern
- Ansätze und Grundsätze der Eingabevalidierung

Kursinhalt

- Grundlagen der Cybersicherheit
- OWASP API-Sicherheit Top Ten
- API1 Gebrochene Autorisierung auf Objektebene
- API2 Fehlerhafte Authentifizierung
- API3 Gebrochene Objekt-Eigenschaftsebene-Autorisierung
- API4 Uneingeschränkter Ressourcenverbrauch
- API5 Gebrochene Autorisierung auf Funktionsebene
- API6 Uneingeschränkter Zugang zu sensiblen Geschäftsflüssen
- API7 Server Side Request Forgery
- API8 Fehlkonfiguration der Sicherheit
- API9 Unsachgemässe Bestandsverwaltung
- API10 Unsicherer Verbrauch von Wirkstoffen
- Einpacken

API security in Node.js (ASINJS)

Weltweite Trainingscenter





Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3 CH-8304 Wallisellen Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch