REST API, ontwerp, architectuur en beveiliging

Praktijkcursus van 3 dagen - 21u
Ref : REH - Prijs 2024 : € 2 070 excl. BTW

Webservices die voldoen aan de REST-architectuurstijl zorgen voor interoperabiliteit tussen computers op het internet.
Je leert over goede ontwerp- en ontwikkelpraktijken en de bijbehorende tools, maar ook over de meest voorkomende kwetsbaarheden en de beste manieren om u daartegen te beschermen.

PEDAGOGISCHE DOELSTELLINGEN

Na afloop van de opleiding kan de cursist:

Maak kennis met de tools die u ondersteunen van ontwerp tot implementatie en supervisie van uw API's

Inzicht in de bedreigingen voor u API's

De meest voorkomende kwetsbaarheden identificeren

De zwakke punten in een API identificeren en vervolgens beschermen

Het beheersen van best practices in het ontwerp, de ontwikkeling en architectuur van ReST API's

HET PROGRAMMA

laatste update: 08/2023

1) Inleiding tot ReST API's

- n-tier architecturen, applicaties en API's.
- De belangrijkste verschillen tussen een REST API en een SOA API.
- H.A.T.E.O.A.S. Bronbeheer en hypermedia links.

Ontwerp van een flexibele, schaalbare, veerkrachtige en krachtige API.

2) Beste praktijk

- Conventies en beste praktijken.
- Versioneringstechnieken en -strategieën.
- Goede benaderingen voor ontwerp en ontwikkeling.

Definitie en ontwerp van een ReST API.

3) De gereedschapskist

- ReST API's ontwerpen met OpenAPI en Swagger.
- Gebruik van Postman of Insomnia.
- Testomgeving en tools (JSON Generator. JSON Server).
- API Mock.

Een ReST API specificeren met Swagger. Een ReST API implementeren en testen.

4) Veiligheidsherinnering

- De belangrijkste principes van IT-beveiliging. Bedreigingen en potentiële impact.
- Specifieke API's: Farming en Throttling.
- BFA en AI: de nieuwe bedreigingen.
- De verschillende injecties (XSS, BSI, XSRF, RFI, XPi, enz.).
- Blootstelling van gevoelige gegevens. Toegang beveiligen.
- Onveilige deserialisatie. Kwetsbare componenten.

DEELNEMERS

Front-end en back-end webontwikkelaars, architecten.

VOORAFGAANDE VEREISTEN

Kennis van HTTP en webontwikkeling: JavaScript/HTML.

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, …
De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

• De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
• Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
• Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN -TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

- Registratie en bewaking.
- Presentatie van de OWASP TOP 10.
- Ontdek Pentesting.
- Inleiding tot Restler-Fuzzer.

Presentatie van een aantal beveiligingsoplossingen voor websites.

5) Authenticatie en autorisatie

- Authenticatiebeveiliging.
- Logsysteem.
- Server-side beveiliging.
- Canonicaliseren, ontsnappen en saneren.
- Toestemmingsbeheer: Rolgebaseerde toegang vs. Resourcegebaseerde toegang.
- CORS (Cross-Origin Resource Sharing) en CSRF (Cross-Site Request Forgery).
- Authenticatie met OAuth2 en OpenID Connect: vocabulaire en workflow.

Zoek en misbruik kwetsbaarheden in authenticatie en autorisatie.

6) Middleware en JWT (JSON Web Token)

- Een herinnering aan cryptografie.
- De belangrijkste principes van JWT.
- Intrinsieke risico's en kwetsbaarheden.

Uitdaging op een onbeveiligde API.

7) API-tests

- De 10 gebieden van API-tests.
- Voordelen en beperkingen van eenmalige API-tests.
- Een API bouwen die testbaar is door het ontwerp.
- Hardingstesten.
- API-conformiteitstestvereisten.
- Bewezen methodes om testkosten te verlagen.

Een API testen met Postman, een Data Driven testscenario maken en CLI-integratie in Newman.

8) API-beheer

- De voordelen van API Management oplossingen.
- Gravitee: moderne, efficiënte opensource APIm.
- API-toegangsbeheer, API-ontwerp, API-beheer, API-implementatie en API-observeerbaarheid.

Gebruik een API-beheeroplossing om een API te implementeren.

DATA

Neem contact met ons op