REST API, conception, architecture et sécurité

Cours Pratique de 3 jours - 21h
Réf : REH - Prix 2024 : 2 070CHF HT

Les services web conformes au style d'architecture REST établissent une interopérabilité entre les ordinateurs sur Internet. Vous pourrez découvrir les bonnes pratiques de conception, de développement, les outils associés ainsi que les vulnérabilités les plus communes et les meilleurs moyens de s'en prémunir.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Prendre en main les outils qui vous accompagneront de la conception au déploiement et la supervision de vos APIs

Appréhender les menaces auxquelles s'exposent vos API

Identifier les vulnérabilités les plus fréquentes

Repérer les points faibles d'une API puis la protéger

Maitriser les bonnes pratiques de conception, de développement et d'architecture des APIs ReST

LE PROGRAMME

dernière mise à jour : 01/2024

1) Introduction aux APIs ReST

- Architectures n-tiers, applications et API s.
- Les différences essentielles entre une API REST et une API SOA.
- H.A.T.E.O.A.S. Gestion des ressources et liens hypermedia.

Travaux pratiques : Conception d'une API flexible, scalable, résiliente et performante.

2) Bonnes pratiques

- Conventions et bonnes pratiques.
- Techniques et Stratégies de Versioning.
- Bonnes approches de conception et de développement.

Travaux pratiques : Définition et conception d'une API ReST.

3) La boîte à outils

- API Mock.
- Conception d'APIs ReST avec OpenAPI et Swagger.
- Utilisation de Postman ou Insomnia.
- Environnement de test et outils (JSON Generator. JSON Server).

Travaux pratiques : Spécification d'une API ReST avec Swagger. Implémentation et test d'une API ReST.

4) Rappels sur la sécurité

- Les grands principes de la sécurité informatique. Menaces et impacts potentiels.
- Spécificités des APIs : Farming et Throttling.
- BFA et IA : les nouvelles menaces.
- Les différentes injections (XSS, BSI, XSRF, RFI, XPi,…).
- Exposition de données sensibles. Sécurisation des accès.

PARTICIPANTS

Développeurs Web Front-end et Back-end, architectes.

PRÉREQUIS

Connaissances HTTP ainsi que des connaissances en développement web : JavaScript/HTML.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Désérialisation non sécurisée. Composants vulnérables.
- Logging et monitoring.
- Présentation de l'OWASP TOP 10.
- Découvrir le Pentesting.
- Introduction à Restler-Fuzzer.

Travaux pratiques : Présentation de quelques solutions de sécurisation de sites web.

5) Authentification et autorisation

- Sécurité de l'authentification.
- Système de logging.
- Sécurité côté serveur.
- CORS (Cross-Origin Resource Sharing) et CSRF (Cross-Site Request Forgery).
- Canonicalization, Escaping et Sanitization.
- Gestion des permissions : Role-Based Acces vs. Resource-based access.
- Authentification avec OAuth2 et OpenID Connect : vocabulaire et workflow.

Travaux pratiques : Recherche et exploitation de vulnérabilités d'authentification et d'autorisation.

6) Middleware et JWT (JSON Web Token)

- Rappels sur la cryptographie.
- Les grands principes de JWT.
- Risques et vulnérabilités intrinsèques.

Travaux pratiques : Challenge sur une API non sécurisée.

7) Les Tests d'API

- Les 10 domaines de tests d'une API.
- Avantages et limites des tests d'API one shot.
- Construire une API Testable by design.
- Les tests de durcissement.
- Les exigences en tests de conformité d'API.
- Les pratiques éprouvées pour réduire les coûts des tests.

Travaux pratiques : Tests d'une API avec Postman, création d'un scénario de test Data Driven, et intégration CLI dans Newman.

8) API Management

- Les avantages des solutions d'API Management.
- Gravitee : APIm opensource moderne et efficace.
- API Access Management, API Design, API Management, API Deployment et API Observability.

Travaux pratiques : Utiliser une solution d'API Management pour déployer une API.

LES DATES

CLASSE À DISTANCE
2024 : 29 mai, 25 sept., 18 nov.