REST API, bonnes pratiques et sécurité

Cours Pratique de 3 jours
Réf : REH - Prix 2022 : 2 050€ 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

Découvrir les menaces auxquelles s'exposent vos API

Découvrir les vulnérabilités les plus fréquentes

Savoir repérer les points faibles d'une API puis la protéger

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

LE PROGRAMME

dernière mise à jour : 06/2021

1) Introduction aux APIs ReST

- L'écosystème moderne.
- Roy Thomas FIELDING : père du ReST.
- Richardson's maturity model ou Web Service Maturity Heuristic.
- H.A.T.E.O.A.S., Resource Linking and Semantic Web.

2) Conventions et bonnes pratiques

- Pragmatisme, idéologie et ReSTafarians.
- Les conventions.
- Les différentes approches de versioning.
- Tips, tricks et bonnes pratiques de conception et de développement.
- Les "standards" ou presque.

Travaux pratiques : Conception d'une API ReST.

3) La boîte à outils

- Conception d'APIs ReST avec OpenAPI et Swagger.
- Debug et testing avec Postman.
- Sandbox. JSON Generator. JSON Server.

Travaux pratiques : Spécification d'une API ReST avec Swagger. Test d'une API ReST avec Postman. Implémentation d'une API ReST.

4) Rappels sur la sécurité

- Menaces et impacts potentiels.
- Les 4 principes de la sécurité informatique.
- Présentation de l'OWASP TOP 10.

PARTICIPANTS

Développeurs Web Front-end et Back-end, architectes, chefs de projet techniques.

PRÉREQUIS

Connaissances HTTP, bonne culture Web. Idéalement quelques 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.

5) Authentification et autorisation

- Sécurité de l'authentification. Cookies are evil.
- CORS et CSRF. Anti-farming et rate-limiting (ou throttling).
- Autorisation et gestion des permissions.
- Les différents niveaux de granularité des mécanismes de gestion de permissions.
- Role-Based Access Control versus Resource-Based Access Control.
- OAuth2 et OpenID Connect.

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

6) Autres vulnérabilités

- Canonicalization, Escaping et Sanitization.
- Injection (code, SQL, NoSQL, données...).
- Data ou cache Poisoning. ReDoS.

Travaux pratiques : Recherche et exploitation de vulnérabilités avec Websheep.

7) J.W.T.

- Rappels sur la cryptographie.
- J.O.S.E. : J.W.K., J.W.S., J.W.E et J.W.T.
- J.W.T. : fonctionnement, risques associés et bonnes pratiques. Vulnérabilités J.W.T.

Travaux pratiques : Recherche et exploitation de vulnérabilités avec Websheep.

8) API Management

- Intérêts et fonctionnalités des solutions d'API Management.
- API management dans le Cloud avec Apigee.
- API management On Premise avec Kong.

LES DATES

BREST
2022 : 27 juil., 26 oct.

CLERMONT-FERRAND
2022 : 29 août, 19 déc.

AIX-EN-PROVENCE
2022 : 31 août, 10 oct., 02 nov.

ANGERS
2022 : 11 juil., 03 oct.

BORDEAUX
2022 : 17 août, 17 oct., 07 nov.

BRUXELLES
2022 : 11 juil., 03 oct.

DIJON
2022 : 29 août, 19 déc.

GENÈVE
2022 : 11 juil., 03 oct.

GRENOBLE
2022 : 29 août, 19 déc.

LILLE
2022 : 11 juil., 05 sept., 07 nov.

LIMOGES
2022 : 17 août, 17 oct.

LUXEMBOURG
2022 : 11 juil., 03 oct.

LYON
2022 : 29 juin, 29 août, 19 sept., 19 déc.

MONTPELLIER
2022 : 31 août, 10 oct.

NANCY
2022 : 29 août, 19 déc.

NANTES
2022 : 27 juil., 26 oct., 07 déc.

NIORT
2022 : 17 août, 17 oct.

ORLÉANS
2022 : 11 juil., 03 oct.

PARIS LA DÉFENSE
2022 : 20 juin, 11 juil., 05 sept., 03 oct., 07 nov., 19 déc.

REIMS
2022 : 11 juil., 03 oct.

RENNES
2022 : 27 juil., 26 oct.

ROUEN
2022 : 11 juil., 03 oct.

SOPHIA-ANTIPOLIS
2022 : 31 août, 10 oct., 02 nov.

STRASBOURG
2022 : 27 juil., 26 oct., 07 déc.

TOULON
2022 : 31 août, 10 oct.

TOULOUSE
2022 : 17 août, 17 oct., 07 nov.

TOURS
2022 : 11 juil., 03 oct.

CLASSE A DISTANCE

2022 : 20 juin, 11 juil., 05 sept., 03 oct., 07 nov., 19 déc.