Tél : (+33)1 55 60 76 72
Email : formation@oxiane.com

APIs ReST Conception, Architecture et Sécurité

APIs ReST Conception, Architecture et Sécurité

Les architectures modernes (Progressive Web Apps, I.o.T., ReST everywhere, MicroServices, etc...) ainsi que la tendance vers la décentralisation et l'interopérabilité ont permis aux APIs ReST de s'imposer comme style d'architecture permettant de véhiculer les données à travers différents services.
En l'absence de standard, l'implémentation d'APIs ReST est un réel challenge nécessitant l'adoption de nombreuses conventions et bonnes pratiques issues de multiples sources et retours d'expérience ainsi que certaines spécifications qui révolutionnent ce domaine.
La mise en place d'APIs ReST est également accompagnée de nouveaux risques de sécurité mais pas de panique !
Cette formation vous permettra de découvrir les bonnes pratiques de conception, de développement et d'architecture des APIs ReST, les outils associés ainsi que les vulnérabilités les plus communes puis surtout les meilleurs moyens de s'en prémunir.

Détails

- Code : AE-RESS
- Durée : 3 jours (21 heures)

Public
- Chefs de projets
- Développeurs

Pré-requis
- Posséder une expérience en développement web : JavaScript, HTTP, HTML
- Etre curieux des technologies Web

Objectifs
- Découvrir les bonnes pratiques de conception, de développement et d'architecture des APIs ReST
- Découvrir et 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 APIs
- Savoir repérer les points faibles d'une API
- Découvrir les vulnérabilités les plus fréquentes, savoir les corriger et développer de façon sécurisée

Programme

Introduction aux APIs ReST

L'écosystème moderne

Roy Thomas FIELDING : Papa du ReST

Richardson's maturity model or Web Service Maturity Heuristic

H.A.T.E.O.A.S., Resource Linking & Semantic Web

Conventions & 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

- Définition et conception d'une API ReST

La Boîte à Outils

Conception d'API ReST avec OpenAPI & Swagger

Debug et testing avec Postman

Sandbox

JSON Generator

JSON Server

Travaux Pratiques

- Spécification d'une API ReST avec Swagger
- Testing d'une API ReST avec Postman
- BONUS : Implémentation d'une API ReST

Rappels sur la Sécurité

Menaces et impacts potentiels

Les 4 principes de la sécurité informatique

Présentation de l'OWASP TOP 10

Authentification et Autorisation

Sécurité de l'authentification

Cookies are evil

CORS (CrossOrigin Resource Sharing)

CSRF (CrossSite Request Forgery)

Antifarming et ratelimiting (ou throttling)

Autorisation et gestion des permissions

Les différents niveaux de granularité des mécanismes de gestion de permissions

RoleBased Access Control vs. ResourceBased Access Control

OAuth2

OpenID Connect

Travaux Pratiques

- Recherche et exploitation de vulnérabilités d'authentification et d'autorisation avec Websheep

Autres vulnérabilités

Canonicalization, Escaping et Sanitization

Injection

Data or Cache Poisoning

ReDoS

Travaux Pratiques

- Recherche et exploitation de vulnérabilités avec Websheep

J.W.T.

Rappels sur la cryptographie

J.O.S.E.

J.W.T. : Fonctionnement, risques associés et bonnes pratiques

Vulnérabilités J.W.T.

Travaux Pratiques

- Recherche et exploitation de vulnérabilités avec Websheep

API Management

Intérêts et fonctionnalités des solutions d'API Management

Apigee

Kong

Modalité

- Stage pratique en présentiel
- Stage pratique en distanciel
- Nombre de stagiaires minimum : 4
- Nombre de stagiaires maximum : 10

Méthodes pédagogiques

- Exposés
- Cas pratiques
- Echanges d'expérience

Profils des intervenants

- Toutes nos formations sont animées par des consultants-formateurs expérimentés et reconnus par leurs pairs.

Modalités d'évaluation

- Evaluation des acquis de la formation par le biais de cas pratiques et/ou mises en situation.
- Attestation de formation remise à chaque participant.

Démarche qualité

- Questionnaire d'évaluation de satisfaction à chaud complété par chaque participant à l'issue de la formation.

Moyens pédagogiques

- Salle équipée de PC (1 poste par stagiaire), vidéo-projecteur.
- Espace de pause.

Dernière mise à jour le 04/02/2021