Tél : +352 27 39 351
Fax : +352 27 39 52 68
Email : formation@oxiane.lu

API ReST : Conception, Bonnes Pratiques, Testing 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-PAPI
- Durée : 3 jours (21 heures)

Public
- Chefs de projets
- Developpeurs

Pré-requis
- Être curieux des technologies Web

  Posséder une expérience en développement web : JavaScript, HTTP, HTML

Objectifs
- Javascript
- Découvrir les enjeux de la gouvernance d'APIs et les outils associés
- Apprendre à consommer une API
- Apprendre à concevoir une API conformément aux conventions et bonnes pratiques
- Apprendre à définir une stratégie de testing adaptée et l'appliquer

Programme

Conception
- De la thèse de Roy T. Fielding au modèle de maturité de Richardson : que retenir ?
- Service-Oriented Architecture (SOA) vs Resource-Oriented Architecture (ROA) vs ReST
- H.A.T.E.O.A.S. & Resource Linking
- *Exercice : Conception d'une API flexible, scalable, résiliente et performante*
- Conventions, Bonnes Pratiques et ReSTafarianisme
- *Exercice : Spécification d'une API avec OpenAPI 3*
- Documentation
- Fakes are not Mocks
- Sandbox
- *Exercice : Développement d'une Sandbox à partir de la spécification OpenAPI*
- Workflow de développement d'une API ReSTful
- Techniques et Stratégies de Versioning
- API vs SDK

Testing
- Les différents types de test
- Pyramide de Tests vs. le Testing en Cornet de Glace
- *Exercice : Testing avec Postman*
- *Démo : Unit Testing*

Sécurité
- Les principaux risques sécurité : OWASP API TOP 10
- *Exercice : Exploitation de vulnérabilités sur une API vulnérable*
- Authentification vs Autorisation
- Les différentes méthodes d'authentification
- Les flows OAuth2.1
- *Exercice : Mise en place d'un Authorization Server / Identity Provider*
- *Exercice : Génération d'un token Machine to Machine (Client Credentials)*
- *Démo ou Exercice : Génération d'un token utilisateur (Implicit Flow)*
- JWT : Fonctionnement, risques associés et bonnes pratiques
- OpenID Connect
- OpenAPI Security Schemes : le point de convergence entre OpenAPI, OAuth2.1 et OpenID Connect
- *Démo : Gestion automatique des autorisations à partir de la spécification OpenAPI*

Gouvernance
- Stratégies de gouvernance
- Style Guide
- *Démo : Validation automatique du style guide*
- Rôle et composantes de l 'API Management
- *Démo d'une solution d'API Management*
- *Exercice : Sécurisation d'une API avec la solution d'API Management Apigee*

Tél : +352 27 39 351
Fax : +352 27 39 52 68
Email : formation@oxiane.lu

- *Démo : Mise en place d'un portail développeur, sécurisation d'une API avec OAuth2, debug et monitoring*

Modalités

- Type d'action :Acquisition des connaissances
- Moyens de la formation :Formation présentielle – 1 poste par stagiaire – 1 vidéo projecteur – Support de cours fourni à chaque stagiaire
- Modalités pédagogiques :Exposés – Cas pratiques – Synthèse
- Validation :Exercices de validation – Attestation de stages