Conception, architecture et sécurité des APIs ReST

La formation "Conception, architecture et sécurité des APIs ReST" vous permettra de découvrir les bonnes pratiques de conception, de développement et d'architecture des APIs ReST, de découvrir et prendre en main les outils qui vous accompagneront de la conception au déploiement et la supervision de vos APIs ainsi que les menaces auxquelles elles s'exposent. Cette formation vous permettra également de savoir repérer les points faibles d'une API ainsi que de découvrir les vulnérabilités les plus fréquentes, savoir les corriger et développer de façon sécurisée. Le programme est donné à titre indicatif et sera adapté à vos besoins et votre niveau après audit. N'hésitez pas à nous contacter pour toute demande spécifique.

Pré-requis

Bonne connaissance en développement web : JavaScript ; http, HTML.

Public concerné

Chefs de projets et développeurs.

Durée et tarif de la formation

La durée de la formation varie en fonction des besoins et des objectifs déterminés après audit. Les tarifs sont disponibles sur devis.

Contenu de la formation

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

La Boîte à Outils

Conception d'API ReST avec OpenAPI & Swagger

Debug et testing avec Postman

Sandbox

JSON Generator

JSON Server

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 (Cross-Origin Resource Sharing)

CSRF (Cross-Site Request Forgery)

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 vs. Resource-Based Access Control

OAuth2

OpenID Connect

Autres vulnérabilités

Canonicalization, Escaping et Sanitization

Injection

Data or Cache Poisoning

ReDoS

J.W.T.

Rappels sur la cryptographie

J.O.S.E.

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

Vulnérabilités J.W.T.

API Management

Intérêts et fonctionnalités des solutions d'API Management