Formation Conception, Architecture et Sécurité des APIs ReST

Objectifs de la formation API ReST

REST (Representational State Transfer) est un style d'architecture SOA simplifiée afin de mettre en oeuvre et de consommer des services web en bénéficiant de tous les avantages d'Internet : scalabilité, caching, etc. Cette formation apprend aux architectes /designers/ développeurs à bien concevoir et implémenter leurs APIs ReST afin d'obtenir la meilleure flexibilité, scalibility, performance et sécurité.

Plus concrètement, à l'issue de ce cours vous serez en mesure de:

- Découvrir les bonnes pratiques d'architecture et de design d'APIs ReSTful.
- Découvrir les menaces auxquelles s'exposent vos API.
- Découvrir les vulnérabilités les plus fréquentes.
- Savoir repérer les points faibles d'une API.
- Savoir corriger les vulnérabilités et développer de façon sécurisée.

À qui s'adresse cette formation ?

Public :

Cette formation n'est pas uniquement dédiée aux développeurs Java mais à tous ceux qui ont déjà développés ou qui souhaitent développer des APIs ReST dans les règles de l'art.

Prérequis :

Avant de suivre cette formation REST APIs, il vous faut avoir certaines connaissances en développement Web : JavaScript / HTTP / HTML. Etre curieux des technologies Web est également un plus.

Contenu du cours API ReST

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 (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

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

Bonus : Prise en main de la solution d'API management Kong