

Formation Sécurité des API Rest

Code : SEC-API-100

Durée : 3 jours (21 heures)

Public visé

Développeurs Web Front End et Back End, architectes, chefs de projets techniques.

{{< formation-prerequis >}}

Objectifs pédagogiques

À l'issue de cette formation, vous serez capable de :

- Décrire les bonnes pratiques de conception, de développement et d'architecture des API REST (dans les 4 principaux langages : Python, PHP, Java, .NET)
- Concevoir, déployer et superviser des API
- Identifier les menaces auxquelles s'exposent vos API
- Distinguer les vulnérabilités les plus fréquentes
- Repérer les points faibles d'une API puis la protéger

Programme

Jour 1 - Matin

Introduction aux API REST

- Introduction aux API, évolution, REST vs SOAP, requêtes
- Conventions et bonnes pratiques
- Design Patterns

Travaux pratiques indicatifs

- Création API météo

Jour 1 - Après-midi

Outils

- OpenAPI, Swagger, Postman, Sandboxing, JSON Generator

Travaux pratiques indicatifs

- Test et validation d'implémentation

Jour 2 - Matin

Sécurité des API - Les fondamentaux

- Rappels sécurité, menaces, principes, OWASP top 10, évolution problématiques API

Jour 2 - Après-midi

Sécurité Web appliquée aux APIs

- Authentification, manipulation identifiants, déni service, SSRF, mauvaise configuration, inventaire, API tierces, développement

Travaux pratiques indicatifs

- Audit API vulnérable

Jour 3 - Matin

Authentification et autorisation

- OAuth2, OpenID Connect, sécurité serveur, permissions, journalisation

Jour 3 - Après-midi

Middleware et cryptographie

- JWT, cryptographie, principes, risques

Travaux pratiques indicatifs

- Création API sécurisée

Modalités d'évaluation des acquis

En cours de formation, par des études de cas ou des travaux pratiques. En fin de formation, par un questionnaire d'auto-évaluation.

{{< formation-require >}}

{{< formation-seealso >}}