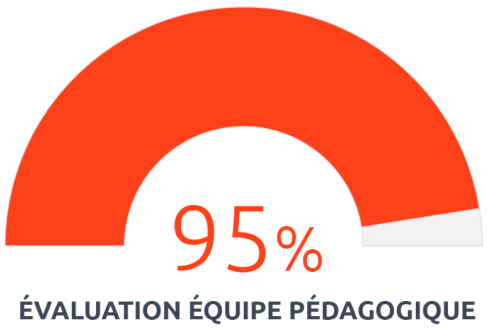
Les-Tilleuls.coop

PROGRAMME DE FORMATION

Concevoir son API HTTP avec REST



OBJECTIFS

Le web est conçu comme un système hypermédia distribué à l'échelle d'internet : apprenez à tirer parti des standards du web pour votre API.

À l'issue de la formation, le participant ou la participante sera en mesure de :

- Sélectionner les standards et approches les plus pertinentes pour concevoir son API
- Concevoir le modèle publique de son API au plus près des standards du web
- Sélectionner les outils qui vous accompagneront de la conception au déploiement et la supervision de vos APIs
- Se prémunir des menaces auxquelles s'exposent vo

PRÉ-REQUIS

- ➔ Ordinateur portable à apporter
- ➔ Docker et Docker Compose à jour

PUBLIC VISÉ

Développeuses et développeurs PHP.

DURÉE

3 jours.

MOYENS ET MÉTHODES PÉDAGOGIQUES

- Présentation des concepts théoriques.
- Ateliers avec cas pratiques.

MODALITÉS D'ÉVALUATION

- Diagnostic préalable à l'inscription
- Evaluation en contrôle continue (ateliers et exercices pendant la formation)
- QCM en fin de formation

PROGRAMME

Introduction aux APIs REST

- L'écosystème moderne.
- La naissance du web et du REST.
- Richardson's maturity model ou Web Service Maturity Heuristic.
- H.A.T.E.O.A.S., Resource Linking and Semantic Web.

Conventions et bonnes pratiques

- Pragmatisme et idéologie.
- Les conventions.
- Les différentes approches de versioning.
- Tips, tricks et bonnes pratiques de conception et de développement.
- Les "standards".

Outillage

- Documentation d'APIs REST avec OpenAPI.
- Découverte des outils de publication de documentation.
- Debug et testing avec Postman.
- API Mock.
- Intérêts et fonctionnalités des solutions d'API Management.

Rappels sur la sécurité

- Menaces et impacts potentiels.
- Les 5 principes de la sécurité informatique.
- Présentation de l'OWASP TOP 10.

Authentification et autorisation

- Sécurité de l'authentification. Cookies are evil.

- CORS et CSRF. 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 versus Resource-Based Access Control.
- OAuth2 et OpenID Connect.

Autres vulnérabilités

- Canonicalization, Escaping et Sanitization.
- Injection (code, SQL, NoSQL, données...).
- Data ou cache Poisoning. ReDoS.

Authentification & Autorisation

- Rappels sur la cryptographie (RSA).
- J.O.S.E. : J.W.K., J.W.S., J.W.E et J.W.T.
- J.W.T. : fonctionnement, risques associés et bonnes pratiques. Vulnérabilités J.W.T.

NOTES

Nous pouvons ajuster la formation à vos besoins, en mettant l'accent sur un aspect plus particulier du développement.

PSH

Les personnes en situation de handicap sont invitées à contacter en toute confidentialité notre équipe pour définir les modalités d'accueil de la formation **PSH@les-tilleuls.coop**.