ReST API, bonnes pratiques et sécurité

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Éligible au CPF : Non

Domaine : Cybersécurité - sécurité informatique

Action collective : Non

Filière : Fondamentaux de la cybersécurité

Rubrique : Fondamentaux

PRÉSENTATION

Objectifs & compétences

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

Public visé

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.

Pré-requis

Connaissances en développement Web : JavaScript / HTTP / HTML.

PROGRAMME

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

Code de formation : R-SPI

€ Tarifs

Prix public : 1980 €

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Durée : 21 heures

Délai d'accès : Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

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

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.
Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.
Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.
Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels.

Méthode

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.
Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.