

Sessions garanties disponibles

Formation API REST : concevoir, sécuriser et industrialiser ses API

Réf. SF33626

Maîtrisez le cycle complet d'une API REST de qualité production : de la conception design-first à la défense contre les attaques de l'OWASP API Security Top 10.

3 j Durée	2 100 € HT Inter / participant	3 500 € HT Intra (≤12 pers.)	87 Sessions à venir
--------------	-----------------------------------	---------------------------------	------------------------

Objectifs pédagogiques

- ✓ Concevoir une API REST conforme aux conventions du métier (ressources, versioning, gestion d'erreurs)
- ✓ Diagnostiquer les vulnérabilités d'une API au regard de l'OWASP API Security Top 10
- ✓ Spécifier une API en approche design-first avec OpenAPI et Swagger
- ✓ Sécuriser une API contre les menaces courantes (BOLA, injections, SSRF, abus de ressources)
- ✓ Implémenter l'authentification et l'autorisation avec OAuth2, OpenID Connect et JWT
- ✓ Automatiser les tests d'une API et l'exposer via une passerelle d'API Management

Public visé & prérequis

Public visé Développeurs

Prérequis- Maîtriser les bases du protocole HTTP (verbes, codes de statut, en-têtes) - Être à l'aise avec le format JSON - Avoir une expérience du développement web (quel que soit le langage serveur)

Programme détaillé

Architecture REST et anatomie d'une API de qualité

- Style REST : principes (ressources, représentations, sans état) et place dans une architecture n-tiers
- Verbes HTTP et codes de statut : sémantique correcte et erreurs courantes à éviter
- Niveaux de maturité (Richardson) et HATEOAS : repères pour situer une API, sans dogmatisme
- REST face aux alternatives : positionnement vis-à-vis de SOAP (legacy) et aperçu de GraphQL/gRPC
- Critères d'une « bonne » API : lisibilité, prévisibilité, évolutivité

Activités pratiques :

- Lecture critique d'une API publique : repérer les bons et mauvais choix de conception
- Cartographie des ressources et des endpoints d'un cas métier

Conventions de conception et stratégies de versioning

- Nommage des ressources et structuration des URI : conventions partagées du métier
- Pagination, filtrage, tri : patterns standards pour les collections volumineuses
- Gestion des erreurs : formats normalisés (problem+json) et messages exploitables côté client
- Stratégies de versioning : URI, en-tête, media-type — arbitrages et impacts
- Idempotence et cohérence : fiabiliser les écritures et les jeux

Activités pratiques :

- Conception complète du contrat d'une API REST sur un cas métier
- Revue par les pairs des choix de versioning et de gestion d'erreurs

Spécification design-first avec OpenAPI

- Approche design-first : spécifier avant de coder pour aligner équipes et consommateurs

- OpenAPI 3.x : structure d'un contrat, schémas, paramètres, réponses
- Swagger et outillage : génération de documentation et de mocks
- Mocks et environnements de test : JSON Server, sandbox, données simulées
- Postman / Insomnia : explorer, requêter et documenter une API

Activités pratiques :

- Rédaction d'un contrat OpenAPI complet et génération de la documentation
- Mise en place d'un mock server pour tester sans back-end

Fondamentaux de sécurité et OWASP API Security Top 10

- Surface d'attaque d'une API : en quoi elle diffère d'une application web classique
- Principes de sécurité : confidentialité, intégrité, disponibilité, traçabilité
- OWASP API Security Top 10 (2023) : panorama des risques majeurs et exemples concrets
- Abus de ressources et déni de service : throttling, rate-limiting, quotas
- Menaces automatisées : force brute, scraping et outillage offensif (cadre concret)

Activités pratiques :

- Analyse de risques d'une API existante au regard de l'OWASP API Security Top 10
- Mise en place d'une stratégie de rate-limiting sur un endpoint sensible

Authentification et autorisation

- Authentification vs autorisation : distinguer les deux et leurs pièges
- OAuth2 : flows (authorization code, client credentials) et cas d'usage
- OpenID Connect : authentification déléguée et jetons d'identité
- Contrôle d'accès : RBAC vs ABAC / Resource-Based Access Control
- Failles d'autorisation : BOLA et accès non maîtrisé aux objets (risque n°1 de l'OWASP API)
- CORS et CSRF : comportements, bonnes configurations et erreurs fréquentes

Activités pratiques :

- Mise en œuvre d'un flow OAuth2 / OpenID Connect sur l'API fil rouge
- Recherche et exploitation d'une faille d'autorisation (type BOLA) sur une API volontairement faillible

Jetons JWT et cryptographie appliquée

- Rappels de cryptographie : signature, chiffrement, gestion des clés
- JOSE et structure d'un JWT : en-tête, payload, signature
- Vulnérabilités JWT : alg=none, confusion d'algorithme, clés faibles, fuite de jeton
- Bonnes pratiques : durée de vie, rotation, stockage et révocation des jetons

Activités pratiques :

- Mise en place d'une authentification par JWT
- Exploitation puis correction d'une vulnérabilité JWT classique

Autres vulnérabilités et tests d'API automatisés

- Injections et désérialisation : vecteurs côté API et parades
- Cache poisoning, SSRF, ReDoS : mécanismes et mesures préventives
- Tests d'API : domaines à couvrir et conception d'une API « testable by design »
- Automatisation : scénarios de test avec Postman, exécution en CLI avec Newman
- Intégration continue : intégrer les tests d'API au pipeline pour prévenir les régressions

Activités pratiques :

- Construction d'une suite de tests data-driven et exécution via Newman
- Audit d'une API faillible : identifier, exploiter puis corriger les vulnérabilités

Exposition et exploitation via l'API Management

- Rôle d'une passerelle d'API Management : sécurité, quotas, observabilité
- Plans, clés d'API et politiques : gérer l'accès des consommateurs
- Observabilité : journalisation, métriques et supervision d'une API en production

- Déploiement et cycle de vie : exposer, publier et faire évoluer une API
- Panorama des solutions : Kong, Gravitee et équivalents (au choix du formateur)

Activités pratiques :

- Exposition de l'API fil rouge derrière une passerelle d'API Management
- Configuration de quotas, de clés d'API et de tableaux de bord d'observabilité

Prochaines sessions

DATE	LIEU	STATUT
18/11/2026	à distance	Sur confirmation
18/11/2026	Paris	Sur confirmation
18/11/2026	Nantes	Sur confirmation
18/11/2026	Lille	Sur confirmation
07/12/2026	Lyon	Sur confirmation
07/12/2026	à distance	Sur confirmation

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

4,9/5 — 9 avis

Donatien W. — Formation dense mais très digeste avec beaucoup de points abordés. Les spécificités de chacun ont pu être abordées.

Jean-Baptiste M. — Le format 3 jours est une contrainte forte. A la sortie de cette formation, on attaque à peine la "vallée du doute" et on sent qu'il y a...

Votre formateur

Stéphane R. — Formateur PHP

Stéphane intervient sur des formations portant sur les langages et écosystèmes backend. Parmi les formations qui lui sont confiées figurent notamment « Python » et « API REST : concevoir,...

Ils nous font confiance

Cette année notre filière Architecture & Design Logiciel a accompagné plus de 50 entreprises dont :

SOPRA STERIA CIMPA SAS THALES GLOBAL SERVICES SAS ADEO SERVICES AUBAY LBC FRANCE ORANGE BUSINESS SQLI WORLDLINE FRANCE SAS ADEVINTA +40 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com