Sécurité offensive des API : découverte, exploitation et remédiation

Lien : https://innov-systems.com/formation/securite-offensive-des-api-decouverte-exploitation-et-remediation

DURÉE
5 jours (35h)

RÉFÉRENCE
SI114

CATÉGORIE
Pentest

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les risques et menaces liés aux API modernes
- Identifier et cartographier les API exposées
- Maîtriser les techniques de test offensif des API
- Exploiter les vulnérabilités selon OWASP API Top 10
- Renforcer la sécurité des mécanismes d’authentification et d’autorisation
- Mettre en place des stratégies de protection des API
- Intégrer la sécurité API dans les pipelines DevSecOps
- Améliorer la détection des attaques sur API
- Développer des plans de remédiation efficaces
- Réduire la surface d’attaque des systèmes exposés
- Auditer les API de manière structurée et professionnelle
- Étudier des cas concrets d’attaques et de sécurisation d’API

POUR QUI ?

- Ingénieurs cybersécurité
- Pentesters / Red Teamers
- API developers
- DevSecOps engineers
- Architectes logiciels
- Security engineers
- SOC analysts
- Consultants cybersécurité
- QA engineers spécialisés sécurité
- Product owners techniques
- Cloud engineers
- Toute personne impliquée dans le développement ou la sécurisation des API

Innov Systems

Programme détaillé

1 / Introduction à la sécurité des API

- Rôle central des API dans les architectures modernes
- Surface d’attaque des API REST, GraphQL et gRPC
- Typologie des menaces ciblant les API

2 / Cartographie et découverte des API

- Reconnaissance et inventaire des endpoints
- OSINT et techniques de discovery API
- Analyse des documentations (Swagger, OpenAPI)

3 / Authentification et autorisation des API

- Mécanismes OAuth2, JWT et API Keys
- Gestion des sessions et des tokens
- Failles d’autorisation (BOLA, BFLA)

4 / Tests offensifs des API

- Méthodologies de pentest API
- Injection, manipulation de paramètres et fuzzing
- Tests automatisés et manuels

5 / Vulnérabilités OWASP API Security Top 10

- Identification des principales failles API
- Broken Object Level Authorization (BOLA)
- Exposition excessive de données et manque de rate limiting

Innov Systems

6 / Exploitation des API vulnérables

- Scénarios d’attaque réalistes
- Escalade de privilèges via API
- Exfiltration de données sensibles

7 / Sécurisation des API

- API Gateway et contrôle d’accès centralisé
- Validation des entrées et sanitation
- Throttling et protection contre les abus

8 / Monitoring et détection des attaques API

- Logs et observabilité des API
- Détection des comportements anormaux
- Intégration avec SIEM et SOC

9 / Remédiation et bonnes pratiques

- Correction des failles API critiques
- Sécurisation du cycle de développement (DevSecOps)
- Tests de sécurité continus dans CI/CD

10 / Cas pratiques et exercices offensifs

- Audit complet d’une API REST
- Simulation d’attaque sur API réelle
- Plan de remédiation et durcissement

Innov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

22 au 26 Fév. 2027	Présentiel - Casablanca
19 au 23 Avr. 2027	Présentiel - Casablanca
14 au 18 Juin 2027	Présentiel - Casablanca
09 au 13 Août 2027	Présentiel - Casablanca
04 au 08 Oct. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés