



Hacking avancé des applications web et Infrastructures Modernes

Lien :

<https://innov-maroc.com/formation/hacking-avance-des-applications-web-et-infrastructures-modernes>

 DURÉE
3 jours (21h)

 RÉFÉRENCE
SEC319

 CATÉGORIE
Sécurité des Applications

OBJECTIFS DE LA FORMATION

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

- ✓ Identifier et comprendre les vulnérabilités avancées affectant les applications web modernes
- ✓ Exploiter et corriger des failles complexes issues des dépendances, des API et des environnements cloud
- ✓ Renforcer la sécurité des architectures web en intégrant les meilleures pratiques DevSecOps
- ✓ Mettre en œuvre des stratégies de détection et de remédiation à travers des ateliers pratiques et des audits de sécurité

POUR QUI ?

- ✓ Développeurs confirmés
- ✓ Ingénieurs en cybersécurité
- ✓ Pentesters
- ✓ Responsables techniques et administrateurs systèmes souhaitant approfondir la sécurité applicative et infrastructurelle dans des environnements modernes

INNOV MAROC



Programme détaillé

1 / INTRODUCTION À LA SÉCURITÉ APPLICATIVE AVANCÉE

- Panorama des menaces actuelles dans les environnements web
- Architecture d'une application vulnérable : points faibles et surfaces d'attaque
- Méthodologie de test et exploitation éthique

2 / EXPLOITATION DES FAILLES CACHÉES

- Second-Order Vulnerabilities : attaques différées et exploitations en chaîne
- Prototype Pollution en profondeur (JavaScript et frameworks front-end)
- CRLF Injection et manipulation des entêtes HTTP
- Étude de cas : compromission silencieuse d'applications via entrées persistantes

3 / POSTMESSAGE ET COMMUNICATIONS INTER-DOMAINES

- Risques liés aux échanges entre iframes et domaines distincts
- Techniques d'attaque et stratégies de mitigation
- Mise en pratique : sécurisation d'un module de communication web

4 / ATELIER PRATIQUE - APPLICATION VULNÉRABLE

- Mise en place d'un environnement d'exploitation (Docker, Node.js, Python)
- Découverte, exploitation et correction des vulnérabilités identifiées

5 / SSRF ET ATTAQUES SUR LES SERVICES DISTANTS

- Compréhension et exploitation d'une SSRF dans des environnements cloud
- Attaques via les métadonnées des services AWS, Azure, GCP
- Techniques de détection et durcissement des API exposées

6 / DÉPENDANCES ET SUPPLY CHAIN SECURITY

- Dependency Confusion : attaques sur les dépôts publics (npm, PyPI, Maven)
- Gestion sécurisée des bibliothèques et versions
- Audit et surveillance continue des dépendances (Snyk, OWASP Dependency-Check)

7 / SÉCURITÉ DES TOKENS ET MÉCANISMES D'AUTHENTIFICATION

- JWT : vulnérabilités, falsifications et erreurs de validation
- Bonnes pratiques de signature, rotation et chiffrement
- Détournement de sessions et contre-mesures

8 / ATELIER PRATIQUE - CHAÎNE D'EXPLOITATION

- Création d'un scénario d'attaque complet : SSRF → LFI → JWT compromise
- Application des correctifs et validation par audit automatique

9 / ATTAQUES SUR LES INFRASTRUCTURES ET SERVICES ASSOCIÉS

- Subdomain Takeover : reconnaissance, exploitation et sécurisation DNS
- XXE (XML External Entity) : injections XML et exfiltration de données sensibles
- Cas pratique : exploitation contrôlée et remédiation

10 / SÉCURITÉ DES COMMUNICATIONS ET DES ÉCHANGES

- SPF, DKIM, DMARC : sécurisation des emails contre l'usurpation
- Bonnes pratiques TLS/SSL et configuration des en-têtes HTTP (HSTS, CSP, etc.)
- Implémentation et test des mécanismes de sécurité

11 / STRATÉGIE DE SÉCURISATION ET CULTURE DEVSECOPS

- Intégration continue de la sécurité dans le cycle de développement
- Tests de sécurité automatisés (CI/CD, pipelines)
- Revue d'outils : Burp Suite, OWASP ZAP, Nikto, Nuclei, Trivy

12 / ÉVALUATION FINALE ET ATELIER DE RÉMÉDIATION

- Audit complet d'une application web par les participants
- Analyse des failles découvertes et priorisation des corrections
- Restitution et plan d'action de sécurisation à long terme

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

 21 au 23 Oct. 2026

 Distanciel

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

Réservation & Renseignements

 Téléphone : +212 522 247 210

 Email : contact@innov-maroc.com

 Web : <https://www.innov-maroc.com>