Tests d’Intrusion et Sécurisation des Applications Web Modernes

Lien : https://innov-systems.com/formation/tests-dintrusion-et-securisation-des-applications-web-modernes

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC307

CATÉGORIE
Test d'Intrusions, Techniques de Hacking, Contre Mesures et Audit

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les menaces et vulnérabilités spécifiques aux environnements Web modernes (API, frameworks JS, conteneurs, etc.)
- Maîtriser les techniques d’audit et de tests d’intrusion des applications Web selon les standards OWASP
- Identifier, exploiter et corriger les vulnérabilités les plus critiques
- Mettre en œuvre des contre-mesures efficaces et des pratiques de développement sécurisé
- Acquérir une approche “offensive & défensive” pour renforcer la sécurité applicative en continu

POUR QUI ?

- Développeurs et ingénieurs Web
- DevSecOps et administrateurs systèmes
- Chefs de projet techniques
- Architectes logiciels
- Responsables techniques souhaitant renforcer la sécurité de leurs applications Web

Innov Systems

Programme détaillé

1 / COMPRÉHENSION DES RISQUES ET DU CONTEXTE SÉCURITÉ

- Panorama des menaces Web actuelles et typologies d'attaques
- Impacts métiers et risques liés à la compromission applicative
- Présentation des standards OWASP, ISO et NIST en sécurité applicative

2 / ENVIRONNEMENT DE TESTS ET OUTILLAGE DE PENTEST

- Installation et configuration d'un laboratoire d'audit Web (VM, proxy, Burp, OWASP ZAP)
- Utilisation de proxies HTTPS pour intercepter et modifier le trafic
- Présentation et usage des environnements vulnérables (DVWA, Juice Shop)

3 / RAPPELS TECHNIQUES ESSENTIELS DU WEB

- Fonctionnement du protocole HTTP/HTTPS, entêtes, cookies et statelessness
- Analyse des formulaires, des requêtes POST/GET et des paramètres
- Encodages et formats de données : URL, HTML, Base64, JSON

4 / MÉTHODOLOGIE DE TESTS D'INTRUSION

- Étapes du pentest Web : reconnaissance, cartographie, exploitation, rapport
- Définition du périmètre et gestion éthique / légale du test
- Introduction à la norme PTES

5 / RECONNAISSANCE PASSIVE ET ACTIVE

- Collecte d'informations publiques (Google Dorking, WHOIS, Shodan)
- Crawling et cartographie applicative
- Découverte d'interfaces cachées et endpoints API

Innov Systems

6 / ANALYSE DES MÉCANISMES D’AUTHENTIFICATION

- Identifier les failles d’authentification (brute-force, enumeration, bypass)
- Exploitation manuelle et automatisée avec Hydra et Burp Intruder
- Contre-mesures : MFA, verrouillage, gestion sécurisée des jetons JWT

7 / GESTION DE SESSION ET MAINTIEN D’ÉTAT

- Étude des cookies, jetons, et stockage local
- Attaques de fixation et de vol de session (Session Hijacking)
- Mesures de protection : Secure / HttpOnly, rotation, expiration

8 / CONTRÔLES D’AUTORISATION ET MISES EN DANGER DES PRIVILÈGES

- Attaques horizontales et verticales (IDOR, bypass ACL)
- Démonstration pratique de CSRF, LFI/RFI et Path Traversal
- Bonnes pratiques de contrôle d’accès et validation côté serveur

9 / EXPLOITATION DES ENTRÉES UTILISATEURS

- Injection SQL, NoSQL, LDAP et commande système
- Outils d’automatisation (SQLMap, NoSQLMap)
- Mesures de prévention : ORM, requêtes préparées, validation côté serveur

10 / ATTAQUES DE TYPE CROSS-SITE

- XSS réfléchi, persistant et DOM-based
- Attaques sur les frameworks modernes (React, Angular, Vue)
- Contre-mesures : CSP, escaping, frameworks sécurisés

11 / SÉCURITÉ DU CODE ET DES DONNÉES

- Gestion des erreurs et exceptions
- Stockage sécurisé des informations sensibles

Inov Systems

- Bonnes pratiques de développement sécurisé (secure coding guidelines)

12 / JOURNALISATION ET SURVEILLANCE

- Bonnes pratiques de log applicatif
- Attaques par injection de logs
- Détection d’intrusion et corrélation d’événements de sécurité

13 / SÉCURISATION DES API WEB ET FRONT-END

- Tests de vulnérabilités sur SOAP et REST
- Attaques sur les API (Broken Object Level Authorization, Injection, Rate Limiting)
- Sécurisation via OAuth2, JWT, et CORS

14 / STRATÉGIE DE REMÉDIATION ET INTÉGRATION DANS LE CYCLE DEVSECOPS

- Intégration des tests de sécurité dans la CI/CD
- Automatisation avec OWASP Dependency-Check, Snyk, etc.
- Communication et reporting des vulnérabilités

15 / ÉTUDE DE CAS ET ÉVALUATION FINALE

- Réalisation d’un test d’intrusion complet sur une application cible
- Rapport de vulnérabilités et recommandations de correction
- Quiz et validation des acquis

Inov 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

12 au 18 Jan. 2027	Présentiel - Casablanca
08 au 12 Mars 2027	Présentiel - Casablanca
03 au 07 Mai 2027	Présentiel - Casablanca
28 Juin au 02 Juil. 2027	Présentiel - Casablanca
23 au 27 Août 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