Pentest avancé des applications web : OWASP Top 10, injection, authentification & logique métier

Lien : https://innov-systems.com/formation/pentest-avance-des-applications-web-owasp-top-10-injection-authentification-logique-metier

DURÉE
5 jours (35h)

RÉFÉRENCE
SI111

CATÉGORIE
Pentest

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Maîtriser les méthodologies avancées de pentest web
- Identifier et exploiter les vulnérabilités OWASP Top 10
- Tester la sécurité des mécanismes d’authentification et de session
- Détecter les failles d’injection et de contrôle d’accès
- Analyser les vulnérabilités de logique métier
- Réaliser des tests d’intrusion complets sur applications web
- Exploiter les failles de sécurité de manière contrôlée
- Rédiger des rapports techniques de pentest professionnels
- Proposer des mesures de remédiation efficaces
- Comprendre les impacts business des vulnérabilités web
- Améliorer la posture de sécurité applicative des organisations
- Étudier des cas réels d’attaques web avancées

POUR QUI ?

- Pentesters / Ethical hackers
- Ingénieurs cybersécurité
- SOC analysts
- Développeurs web et backend
- DevSecOps engineers
- Architectes applicatifs
- RSSI / CISO
- Consultants cybersécurité
- QA / testeurs sécurité
- Bug bounty hunters
- Auditeurs sécurité applicative
- Toute personne impliquée dans la sécurité des applications web

Innov Systems

Programme détaillé

1 / Introduction au pentest web avancé

- Rôle du test d'intrusion dans la cybersécurité applicative
- Méthodologies (OWASP Testing Guide, PTES)
- Cycle complet d'un pentest web

2 / Reconnaissance et cartographie d'application web

- Fingerprinting des technologies web
- Analyse des endpoints et surfaces d'attaque
- Outils de reconnaissance (Burp Suite, Nmap, etc.)

3 / OWASP Top 10 et analyse des vulnérabilités critiques

- Présentation des principales vulnérabilités OWASP
- Priorisation des risques applicatifs
- Impact business des failles web

4 / Attaques par injection

- SQL Injection (SQLi)
- Command Injection et OS Injection
- NoSQL Injection et XML Injection

5 / Sécurité de l'authentification et de la session

- Failles d'authentification (brute force, credential stuffing)
- Gestion des sessions et tokens
- JWT attacks et mauvaise implémentation OAuth

Innov Systems

6 / Contrôle d’accès et escalade de privilèges

- IDOR (Insecure Direct Object Reference)
- Broken Access Control
- Vertical et horizontal privilege escalation

7 / Vulnérabilités de logique métier

- Contournement des workflows applicatifs
- Abus de fonctionnalités métier
- Exploitation des erreurs de conception fonctionnelle

8 / Attaques XSS, CSRF et vulnérabilités client-side

- Stored, Reflected et DOM XSS
- CSRF et protections modernes
- Sécurité JavaScript et frameworks front-end

9 / Exploitation avancée et post-exploitation web

- Web shells et persistence
- Extraction de données sensibles
- Chaînage de vulnérabilités

10 / Reporting, remédiation et durcissement

- Rédaction de rapports de pentest
- Recommandations techniques de correction
- Bonnes pratiques de sécurisation des applications web

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

30 Nov. au 04 Déc. 2026	Distanciel
04 au 08 Jan. 2027	Présentiel - Casablanca
01 au 05 Mars 2027	Présentiel - Casablanca
26 au 30 Avr. 2027	Présentiel - Casablanca
21 au 25 Juin 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