



Sécurité Applicative avec PHP

Lien : <https://innov-maroc.com/formation/securite-applicative-avec-php>

 DURÉE
4 jours (28h)

 RÉFÉRENCE
SEC121

 CATÉGORIE
Sécurité des Applications

OBJECTIFS DE LA FORMATION

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

- ✓ Identifier les vulnérabilités les plus courantes des applications Web
- ✓ Comprendre le déroulement d'une attaque
- ✓ Sécuriser efficacement un serveur Web et une application

POUR QUI ?

- ✓ Pentesters et développeurs



Programme détaillé

1 / Introduction

- Statistiques et évolution des failles liées au Web selon IBM X-Force et OWASP
- Evolution des attaques protocolaires et applicatives
- Le monde des hackers

2 / Les constituants d'une application Web

- Les éléments d'une application N-tiers
- Le serveur frontal HTTP, son rôle et ses faiblesses
- Les risques intrinsèques de ces composants
- Les principaux acteurs du marché

3 / Protocole HTTP avec PHP

- Principes d'une application PHP trois tiers
- Requête Ajax
- La fonction header()
- http_response_code()
- Les méthodes HTTP via le module cURL pour PHP

4 / Les risques majeurs des applications Web selon l'OWASP

- Mise en place du Lab
- Introduction au Top 10 OWASP, Top 25 SANS et Veracode

- Les risques majeurs des applications Web selon l'OWASPnjection, LDAP injection...)
- Authentification : Exposition de données sensibles
- XXE (XML eXternal Entity)
- Sécurisation des accès
- Mauvaise configuration de sécurité
- Les attaques "Cross Site Scripting" ou XSS
- Désérialisation non sécurisée
- Composants vulnérables
- Logging et monitoring

5 / Hardening d'une application PHP

- Les forces et faiblesses du langage PHP
- Sécuriser une authentification (captcha et anti-bruteforce PHP)
- Gestion des mots de passe (password_hash / password_verify)
- Renforcement du système de sessions PHP
- Contrôle d'accès (de l'intérêt de la Programmation Orientée Objet en PHP)
- Validation des entrées (filter_var / strip_tags)
- Encodage des sorties (htmlentities / htmlspecialchars)
- Sécuriser un upload de fichier en PHP
- Comment générer des tokens anti-CSRF (Cross Site Request Forgery) ?
- Management des logs (php.ini)

6 / Hardening client / serveur par la pratique

- PHPINFO() / PHPSECINFO()
- php.ini
- CSP (Content Security Policy)
- SOP / CORS
- Tests unitaires PHP
- Analyse statique / dynamique avec RIPS
- Durcissement des trames en PHP

- Ouverture avec l'OWASP testing guide, ASVS (Application Security Verification Standard)

🔧 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

📅 27 au 30 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>

Document généré le 12/10/2026 — Réf : SEC121

INNOV MAROC — Tous droits réservés