Checklist Sécurité Web

Pour agences web & PME marocaines • Édition 2025

Utilisez cette checklist avant chaque mise en production ou audit client.

Chaque point non validé représente un risque potentiel pour votre infrastructure et vos clients.

■ 1. AUTHENTIFICATION & CONTRÔLE D'ACCÈS

- ☐ Mots de passe hashés avec bcrypt ou Argon2 (jamais MD5/SHA1) — CRITIQUE
- ☐ Authentification à deux facteurs (2FA) sur tous les comptes admin — CRITIQUE
- ☐ Politique de mots de passe : min. 12 caractères, majuscule, chiffre, symbole
- ☐ Verrouillage après 5 tentatives échouées (brute-force protection) — OWASP A07
- ☐ Sessions invalidées après déconnexion et expiration automatique (30 min)
- ☐ Rôles et permissions bien définis — principe du moindre privilège
- ☐ Pas de comptes partagés entre collaborateurs

■ 2. SÉCURITÉ HTTP & TRANSPORT

- ☐ HTTPS forcé sur tout le site — certificat TLS valide et à jour — CRITIQUE
- ☐ HSTS activé (Strict-Transport-Security: max-age=31536000) — CRITIQUE
- ☐ Redirection automatique HTTP → HTTPS (301)
- ☐ Content-Security-Policy (CSP) configuré pour bloquer XSS — OWASP A03
- ☐ X-Frame-Options: DENY ou SAMEORIGIN (anti-clickjacking)
- ☐ X-Content-Type-Options: nosniff activé
- ☐ Referrer-Policy défini
- ☐ Permissions-Policy configuré (désactiver caméra/micro inutiles)

Checklist Sécurité Web — Suite

Pour agences web & PME marocaines • Édition 2025

■■ 3. PROTECTION DES DONNÉES (CNDP MAROC)

- ☐ Politique de confidentialité conforme à la Loi 09-08 (CNDP Maroc) — CRITIQUE
- ☐ Déclaration à la CNDP si traitement de données personnelles — CRITIQUE
- ☐ Données sensibles chiffrées en base (AES-256 minimum) — CRITIQUE
- ☐ Consentement explicite collecté avant tout tracking/cookies — CNDP
- ☐ Durée de conservation des données définie et documentée
- ☐ Procédure de suppression de données sur demande

■■ 4. CONFIGURATION SERVEUR & INFRASTRUCTURE

- ☐ Versions de CMS/frameworks à jour (WordPress, Laravel, etc.) — CRITIQUE
- ☐ Panel d'administration sur URL non-standard (pas /wp-admin par défaut) — CRITIQUE
- ☐ Firewall applicatif WAF configuré (Cloudflare, ModSecurity…)
- ☐ Accès SSH par clé uniquement — désactiver login par mot de passe — CRITIQUE
- ☐ Ports non nécessaires fermés — scan régulier Nmap
- ☐ Sauvegardes automatiques quotidiennes testées et chiffrées
- ☐ Logs d'accès et d'erreurs centralisés et monitorés
- ☐ Variables d'environnement dans .env — jamais en dur dans le code — CRITIQUE

■ 5. CODE & DÉPENDANCES

- ☐ Validation de toutes les entrées utilisateur côté serveur — CRITIQUE
- ☐ Requêtes SQL paramétrées (aucune concaténation directe) — CRITIQUE