■ Checklist de Sécurité pour Site Internet

■ Accès et authentification

- ■ Utiliser des mots de passe longs, forts et uniques
- ■ Activer la double authentification (2FA) si possible
- ■ Limiter les accès FTP/SSH (restreindre par IP si possible)

■ Serveur et hébergement

- ■ Forcer le HTTPS avec un certificat SSL/TLS valide
- ■ Mettre à jour régulièrement PHP, CMS, plugins et serveur web
- ■ Vérifier les permissions des fichiers (644) et dossiers (755), éviter 777
- ■ Protéger les fichiers sensibles (.htaccess, .env, config)

■■ Protection contre les attaques

- ■ Activer un pare-feu applicatif (WAF) type Cloudflare ou OVH
- ■ Vérifier les protections contre injections SQL et XSS
- ■ Limiter les tentatives de connexion (bruteforce)
- ■ Désactiver l'indexation des dossiers (Apache/Nginx)

■ Sauvegardes

- ■ Effectuer des sauvegardes régulières des fichiers et BDD
- ■ Stocker les sauvegardes hors du serveur principal

■ Surveillance et logs

- ■ Activer et consulter les logs serveur (Apache/Nginx, PHP)
- ■ Surveiller les connexions suspectes
- ■ Mettre en place un outil de monitoring (ex: UptimeRobot)

■ Bonnes pratiques de développement

- ■ Changer les identifiants admin par défaut
- ■ Supprimer les fichiers de test ou anciens backups visibles
- ■ Limiter l'upload de fichiers et vérifier leur type
- ■ Configurer les en-têtes de sécurité (CSP, X-Frame-Options, etc.)