

GUIDE DE BONNES PRATIQUES POUR LES WEBMASTERS



INTRODUCTION

La sécurité est une priorité incontournable pour chaque webmaster. Un site web sécurisé est essentiel non seulement pour protéger les données sensibles des utilisateurs, mais aussi pour maintenir la crédibilité et la réputation de l'entreprise qui le gère.

Avec l'augmentation des cyberattaques et des violations de données, il est crucial de mettre en place des mesures de sécurité rigoureuses afin de garantir la sécurité du site et de ses utilisateurs.



1 SÉCURISATION DE L'INSTALLATION ET DE LA CONFIGURATION

Pourquoi : *L'installation par défaut d'un système, d'un logiciel ou d'un CMS (WordPress, Joomla, Drupal, etc.) présente plusieurs inconvénients majeurs en matière de sécurité, de performance et de personnalisation.*

Comment :

Utiliser la dernière version du CMS : Maintenir le CMS, les thèmes et les plugins à jour pour corriger les failles de sécurité.

Supprimer les fichiers et extensions inutiles : Supprimez les fichiers d'installation (ex: install.php) et désactivez les modules non utilisés.

Désactiver l'affichage des erreurs PHP ou équivalents : Évitez d'afficher les erreurs pour ne pas révéler d'informations sensibles aux attaquants.

Désactiver l'exécution de scripts dans certains dossiers : Bloquez l'exécution des fichiers .php (ou équivalents) dans les fichiers uploads via .htaccess.

Restreindre les permissions des fichiers : Appliquez le principe du moindre privilège (chmod 644 pour les fichiers et 755 pour les dossiers en général).

Désactiver l'accès aux répertoires via le navigateur : Utilisez des fichiers .htaccess ou équivalents.

Désactiver les services et modules inutiles afin de réduire la surface d'attaque en désactivant tout ce qui n'est pas nécessaire.



2 PROTECTION DES COMMUNICATIONS ET D'HÉBERGEMENT

Pourquoi : *chiffrer les données transmises entre le serveur et les utilisateurs afin de prévenir toute interception et garantir leurs protection et leurs disponibilité.*

Comment :

Activer HTTPS avec un certificat SSL/TLS : Fourniture d'un certificat SSL pour garantir des connexions sécurisées en HTTPS.

Configurer correctement les en-têtes de sécurité HTTP comme Content-Security-Policy, X-Content-Type-Options, et Strict-Transport-Security.

Sécuriser les accès FTP : Privilégiez SFTP ou SSH au lieu de FTP classique pour éviter l'interception des identifiants.

Utiliser un hébergement sécurisé : Optez pour un hébergeur avec des protections anti-DDoS, chiffrement des données sensibles et accès sécurisé.

04



3 VEILLER À LA MISE À JOUR RÉGULIÈRE, SAUVEGARDE ET SURVEILLANCE DU SITE

05

Pourquoi : *Les pirates exploitent fréquemment les vulnérabilités des logiciels obsolètes.*

Comment :

Mettre à jour régulièrement le CMS (**WordPress, Joomla, Drupal, etc.**) et les plugins.

Sauvegardez régulièrement la base de données et les fichiers du site selon la règle 3-2-1 : 3 copies, sur 2 supports différents, dont 1 hors site.

Surveiller les activités suspectes : Utilisez des outils de log et d'audit comme WP Security Audit Log ou OSSEC.

Configurer des alertes de sécurité afin de recevoir des notifications en cas de connexion suspecte ou de modifications non autorisées.



4 RENFORCER LA PROTECTION DES ACCÈS ADMINISTRATIFS

Pourquoi : *Les comptes administrateurs sont souvent ciblés lors des attaques.*

Comment :

Utiliser des mots de passe robustes et uniques idéalement générés par un gestionnaire de mots de passe (minimum 12 caractères, avec une combinaison de lettres, chiffres et symboles).

Changer l'URL de connexion par défaut à l'interface d'administration. (Exemple: ne pas utiliser /wp-admin/ pour WordPress).
Activer l'authentification Multi-facteurs (MFA) pour les accès administrateurs.

Filtrez les adresses IP autorisées ou utilisez un VPN pour accéder à l'interface d'administration.

Limiter le nombre de tentatives de connexion et imposer un délai entre les tentatives échouées.

Mettre en place une politique stricte de gestion des privilèges utilisateurs (principe du moindre privilège).

Procéder à une revue régulière des comptes utilisateurs pour détecter et supprimer les comptes inactifs ou non autorisés.

06



5 SE PROTÉGER CONTRE LES ATTAQUES WEB COURANTES

07

Pourquoi : Grâce à l'exploitation des vulnérabilités et les faiblesses de configuration, les pirates peuvent accéder à la base de données ou injecter du code malveillant.

Comment :

Installer un pare-feu applicatif (WAF) pour filtrer le trafic malveillant dans votre serveur web ou allouer ce service depuis votre hébergeur.

Installer des plugins ou activer un système de protection contre les attaques par force brute comme Fail2Ban, WordFence, Sucuri, ModSecurity ou équivalents.

Sécuriser les formulaires web : Implémentez des CAPTCHA et un filtrage des entrées pour éviter le Cross-Site Scripting (XSS) et les injections SQL.

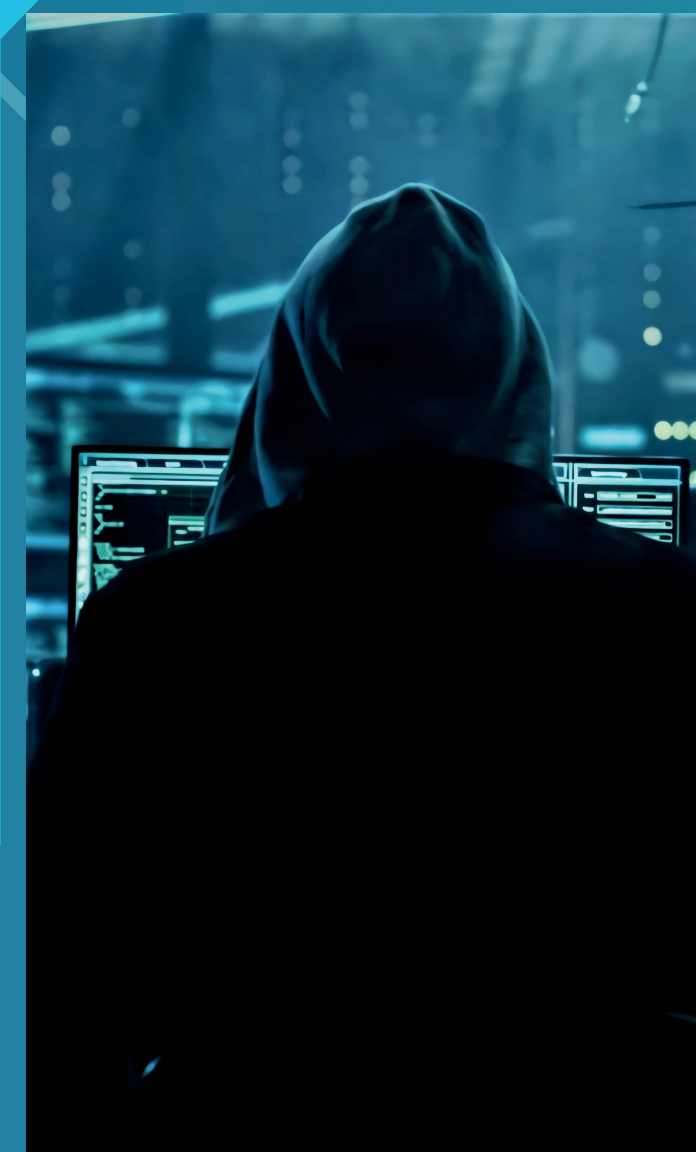
Désactiver l'indexation des répertoires : Ajoutez Options -Indexes dans .htaccess pour empêcher l'accès aux fichiers listés.

Vérifier et nettoyer toutes les données entrantes provenant des utilisateurs en utilisant des bibliothèques de sécurité éprouvées.

Utiliser des tokens CSRF pour empêcher les attaques par falsification de requêtes.

Si nécessaire, limiter les visites à votre site web en fonction du nombre de requêtes client par secondes, par plages d'adresses IP et par pays.

Mettre en place une protection contre les attaques DDoS et implémenter des mécanismes de protection contre le clickjacking via les en-têtes X-Frame-Options.



6 EFFECTUER DES SAUVEGARDES RÉGULIÈRES DU SITE

08

Pourquoi : *Une sauvegarde permet de restaurer le site rapidement en cas de piratage ou de perte de données.*

Comment :

Mettre en place des sauvegardes automatiques quotidiennes ou hebdomadaires.

Effectuer des tests réguliers des sauvegardes afin de garantir leur bon fonctionnement.

Conserver les sauvegardes sur un serveur externe sécurisé, idéalement chiffré et dans une région géographique différente.

Mettre en place une stratégie de rétention des sauvegardes (**quotidiennes, hebdomadaires, mensuelles**).

Documenter clairement la procédure de restauration pour permettre une réponse rapide en cas d'incident.



7 EFFECTUER DES TESTS DE SÉCURITÉ RÉGULIÈREMENT

09

Pourquoi : Anticiper les vulnérabilités pour éviter leurs exploitations.

Comment :

Utiliser des scanners de vulnérabilités avec des outils gratuits comme OWASP ZAP ou Nikto pour identifier les problèmes potentiels avant qu'ils ne soient exploités.

Mettre en place un IDS (Système de Détection d'Intrusion) afin de surveiller le trafic réseau et signaler toute activité suspecte (ex : Snort, Suricata).

Mettre en place un monitoring de disponibilité pour détecter rapidement les interruptions de service.



8 SENSIBILISATION POUR LES WEBMASTERS

10/15

Pourquoi : *Les webmasters jouent un rôle clé dans la sécurité des sites web. Une mauvaise configuration ou un manque de vigilance peut exposer un site à des cyberattaques.*

Comment :

Suivre des formations sur OWASP et les cybermenaces.

Faire des exercices de pentest pour identifier et corriger les vulnérabilités.

Participer à des simulations d'attaques pour tester et améliorer la réaction face aux menaces.

Créer et maintenir à jour un plan de réponse aux incidents de sécurité.

Rester informé des dernières tendances et menaces en cybersécurité via le site web officiel et les réseaux sociaux de l'ANCS.

Participer à des communautés de sécurité pour partager les connaissances et les bonnes pratiques



9 SÉCURITÉ DES API ET DES SERVICES TIERS

Pourquoi : Les API et services tiers peuvent constituer des points d'entrée privilégiés pour les attaquants s'ils ne sont pas correctement sécurisés.

Comment :

Utiliser des mécanismes d'authentification robustes pour les API (OAuth 2.0, JWT).

Mettre en place une limitation de débit (rate limiting) pour prévenir les abus.

Valider rigoureusement toutes les entrées et sorties des API.

Vérifier régulièrement la sécurité des services tiers intégrés à votre site.

Utiliser des clés API distinctes pour différents environnements (Développement, production).

Limiter les autorisations accordées aux services tiers au strict minimum nécessaire.

Surveiller et journaliser toutes les activités des API pour détecter les comportements anormaux.



SYNTHÈSE

12

- 1 *Sécurisation de l'installation et de la configuration*
- 2 *Protection des communications et d'hébergement*
- 3 *Veiller à la mise à jour régulière, Sauvegarde et surveillance du site*
- 4 *Renforcer la protection des accès administratifs*
- 5 *Se protéger contre les attaques web courantes*
- 6 *Effectuer des sauvegardes régulières du site*
- 7 *Effectuer des Tests de sécurité régulièrement*
- 8 *Sensibilisation pour les webmasters*
- 9 *Sécurité des API et des services tiers*



 (+216) 71 846 020 / (+216) 71 843 200

 sensibilisation@ancs.tn

 www.ancs.tn