FICHE OUTIL :

WORDPRESS ET LA SECURITE

Les CMS sont 3 fois plus attaqués que les autres sites. WordPress représente 59,1% des CMS, et il est open source, toute personne aguerrie a donc accès à son code.
70% des sites sous WordPress ont une vulnérabilité.

Pourquoi hacker un site ?

Par pur vandalisme, pour en tirer un bénéfice (redirection vers une autre page) ou pour une utilisation des ressources via botnet pour une attaque DDoS (Distributed Denial of Service attack attaque par déni de service = saturation du serveur).
Les sites WordPress sont souvent hackés par plugin. On en dénombre 50 000 vulnérables dont 1/5ème par brute force ou par DDoS.
Afin de se protéger, il n'existe pas de recette miracle mais des précautions à prendre pour avoir des niveaux de sécurité :

→ Niveau 1 :

- Mises à jour (updates) à faire dès que possible. Possibilité d'automatiser la chose avec des plugins comme WPAutomatic updates, Easy updates manager ou en modifiant le wp-config.php https://www.siteground.com/tutorials/wordpress/auto-update.htm#default .
- Faire des backups réguliers avec VaultPress, Blog Vault ou encore duplicator.
- Ne pas utiliser un utilisateur nommé admin
- Limiter le nombre de tentatives de connexions par une extension comme login lockdown ou Limit Login Attempts.
- Utiliser des mots de passe sécurisés et pas 123456, admin, toto…
- Choisir un hébergeur fiable.

→ Niveau 2 :

- Enregistrer un nombre minimal d'utilisateurs de type administrateurs.
- Mettre les utilisateurs au niveau le plus bas possible.
- Supprimer les utilisateurs qui n'ont plus lieu d'être.
- Supprimer les plugins qui ne sont pas utilisés.
- Mettre des plugins fiables, c'est-à-dire qui ont moins d'un an et dont la version est testée avec la version de WordPress utilisée.
- S'authentifier grâce à une authentification 2 facteurs (SMS + Login). Les plugins WordFence, JetPack permettent de le faire.

→ Niveau 3 :

- Utiliser httpS, gage de sécurité et facteur de ranking.
- En connexion distante, préférer le SFTP (Secure FTP) au FTP.
- Utiliser la version de php préconisée, PHP7 au jour de la mise à jour de cette fiche.
- Préfixe de base de données : wp_ NON ! modifier impérativement le préfixe de base de données par autre chose (gm_, localuxdriver_…).
- Utiliser des CDN : Content Delivery Network. Ce sont des ressources qui sont puisées sur d'autres serveurs, cela limite les attaques DDoS de notre site.
- Utiliser un ordinateur propre (sans virus) et sécurisé.
- Utiliser des clés de sécurité WordPress (Salts).
- Mettre un firewall comme WordFence.
- Utiliser des outils de scanning : Gravityscan, Sucun, JetPack ou encore la google search console qui nous informe en cas de malware.

→ Niveau 4 :

- ServerLess : Site AWS (comme proposé par Amazon) avec d'un côté la prod et le code pour l'administrateur, et d'un autre côté le contenu accessible par tous. Pas de base de données, pas de vulnérabilités.