Sécurité du site

La sécurité des sites webs sont très importants, pour éviter la fuite d'information, ddos, etc. En 2019 une étude a indiqué que 33 % des 10 millions de sites les plus visités utilisent le CMS WordPress (https://bit.ly/3tI3p9w) . Ce qui le fait devenir une des principales cibles des attaques, car il est démocratisé par les grands groupes mais également par les petits groupes.

Différentes solutions des sécurités à appliquer pour contrer les différentes attaques possibles sur le Web.

Protection du site côté administrateur/backend (tentative de connexion) :

Pour gérer et contenir les attaques, un plugin sous le nom de **« Wordfence »**, va nous permettre d'appliquer un pare feu de sécurité sur notre site. Il protège contre les attaques brutes forces, et plus complexe en appliquant par exemple le blocage temporaire ou permanent d'ip. Sa version freemium suffit amplement pour des sites de petites envergures.

Partie Formulaire et Commentaire :

Cette partie va concerner principalement les formulaires que l'on retrouve sur le site Aneolys, dans la partie pour nous contacter et pour commenter des articles du blog.

Ici l'important est d'éviter le spam principalement pouvant mener à un DDoS réseau (épuiser les ressources du serveur pour le faire tomber) et les liens frauduleux que l'on pourrait retrouver dans les commentaires.

Anti-spam :

Plusieurs solutions ont été combinés pour avoir aucune possibilité de spam qui se trouve être un grand fléau.

1. Mise en place de l'anti spam de Google **« Google ReCaptcha V3 »** qui une fois activé, empêchera les soumissions automatisées des robots malveillants.

2. Mise en place d'un « Honeypot » ou en Français « pot de miel ». Système qui va ajouter des champs fictifs, invisibles pour un humain, mais visibles pour les robots. Le formulaire n'est pas validé si ces champs fictifs sont remplis, ce qui va piéger les robots. Le plugin **« Honeypot for WP Comment »** va nous donner la possibilité simplement de l'intégrer aux formulaires de commentaires des articles du blog.

3. Dernière défense contre les spams, si le robot arrive à contourner le Google ReCaptcha V3 et l'Honeypot, il devra faire face au plugin **« Akismet »**. C'est un service de filtrage du spam qui filtre le spam des commentaires.

Lien frauduleux :

Ce problème va concerner les robots et les humains qui veulent commenter et intégrer des liens redirigeant vers des sites frauduleux ou peu fiables. La solution à été d'installer le plugin **« Comment Link Remove »**, qui va amener l'interdiction d'ajouter des liens dans ces commentaires (suppression automatique des liens)

Partie Serveur HTTP (Apache généralement) :

Concernant le serveur HTTP, on doit faire attention de respecter et intégrer des fonctionnalités de sécurités. Le serveur HTTP correspond au serveur qui va contenir tous les fichiers du site/domaine, et qui va le faire fonctionner/dialoguer avec les internautes en répondant aux requêtes (en utilisant le protocole HTTP) qu'il reçoit.

- **Ne pas mettre l'autorisation 777 à tous les fichiers**, cela donne la possibilité de modifier les fichiers à n'importe qui se connectant sur le serveur (en général utiliser soit 644/640 et pour le fichier wp_config 440)
- Sécuriser les connexions au serveur en passant principalement par une **connexion sous protocole SFTP** (éviter la connexion par protocole FTP, le protocole SFTP bloque la possibilité d'écoute d'une autre machine qui récupérerai alors des données ; de plus jamais de connexion via un réseau wifi public car sniffer de données possible (vol de données))
- Protéction des fichier grâce aux fichiers de configuration du serveur Apache **« .htaccess »** (fichier de configuration des outils utilisant le serveur http apache), modification prise en compte dynamiquement

Les consignes de sécurité essentielles :

- Choisir un bon hébergement
- Mettre à jour régulièrement Wordpress ou les plugins (faire attention aux problèmes de compatibilités et sauvegarder le serveur régulièrement)
- Mot de passe sécurisé pour tous les comptes utilisateurs (éviter les attaques brute force, en n'assignant à aucun compte l'username « admin ». En cas de passage de brute force réussie, cela va ouvrir la porte du site et donner les identifiants des autres comptes)
- Faire des sauvegardes régulières, directement sur l'hébergeur ou manuellement via ftp ou via un plugin qui va le faire (par exemple Duplicator)
- Ne pas télécharger des plugins non mis à jour depuis longtemps (potentiellement infecté ou problème de compatibilité avec les autres plugins)