Wordpress - recommandations de sécurisation

Vous trouverez ci-dessous des informations et recommandations pour accroître la sécurité concernant le CMS Wordpress.

Recommandations

Voici une liste non-exhaustive des modifications a apporter afin de sécuriser au minimum votre site Wordpress :

- **Mettre à jour le core, les plugins et les thèmes** du site fonctionnant sous Wordpress.
- **Modifier le lien d'accès à l'administration** (ex : http://votre_site/bo-securise/ au lieu de de http://votre_site/wp-admin/).
- **Modifier le numéro d'ID** du compte administrateur par autre chose que le numéro 1.
- **Ne pas avoir d'utilisateur nommé admin**
- **Limiter l'accès au fichier XMLRPC.PHP** voir l'interdire, lorsqu'il n'y a pas besoin d'accéder à l'ancienne API de Wordpress. *La nouvelle API n'utilise plus cette méthode.*
- **Modifier les clés de sécurité** (Salt et Sécurity Key par défaut de Wordpress).
- **Protéger contre le brute force** les formulaires d'authentification.
- **Supprimer les numéros de version** dans le code du thème et du core Wordpress.
- **Supprimer les messages d'erreur** sur le formulaire de connexion à l'admistration.
- **Prévoir une mise à jour régulière** des plugins et du core Wordpress au moins 2 fois par mois pour les plugins et régulièrement pour les mises à jour majeures du core de Wordpress (les mises à jour mineures s'effectuant automatiquement depuis la version 4.1 de Wordpress).

Certains plugins Wordpress existent pour vous aider à cela, comme par exemple les plugins Solid Security,Wordfence Security, Sucuri Security ou encore SecuPress qui englobent une grande majorité de ces recommandations.