2023

Securité

5 conseils pour sécuriser votre site web WordPress

Pixel Drop

Pixel Drop

Questions courantes

WordPress est-il sécurisé ?
Absolument ! WordPress est le système de gestion de contenu le plus populaire au monde, et ce résultat n'a pas été obtenu sans prendre au sérieux la question de la sécurité.
La réalité est que la plus grande vulnérabilité de WordPress en matière de sécurité est liée à ses utilisateurs. La plupart des piratages de WordPress sur la plateforme peuvent être évités avec un peu d'effort de la part des personnes qui l'utilise.

Comment puis-je rendre mon site web 100 % sûr ?
Malheureusement, il n'existe pas de solution garantie à 100 % pour sécuriser WordPress. Une bonne sécurité consiste à minimiser les risques. Si quelqu'un essaie de vous vendre une solution sécurisée à 100 %, il est en train de vous escroquer. Vous ne serez jamais totalement en sécurité, mais vous pouvez réduire les risques au minimum.

Mon site web est petit. Dois-je vraiment me préoccuper de la sécurité ?
Il n'est pas nécessaire que votre site web soit de grande taille pour attirer l'attention d'un hacker potentiel. Les hackers voient une opportunité d'utiliser votre site comme un conduit pour rediriger vos visiteurs vers des sites malveillants, envoyer des spams, diffuser des virus ou extraire des donnés sensibles.

Pixel Drop

Limiter les connexions

La méthode d'attaque par force brute exploite la forme la plus simple d'accès à un site : en essayant de deviner les noms d'utilisateur et les mots de passe, encore et encore, jusqu'à ce qu'ils réussissent.

Par défaut, WordPress ne limite pas les tentatives de connexion infructueuses. Sans cette limite, WordPress peut être une cible facile pour les attaques par force brute.

Installez un plugin de sécurité ou **souscrivez à la maintenance de Pixel Drop** pour limiter le nombre de tentatives de connexion échouées sur votre site.

La fonction de protection contre la force brute de la maintenance permet de définir le nombre de tentatives de connexion infructueuses avant qu'un nom d'utilisateur ou une adresse IP ne soit bloquée.

Le blocage empêche temporairement l'attaquant d'effectuer des tentatives de connexion.

Une fois que les attaquants ont été bloqués trois fois, il leur est interdit de consulter le site.

Pixel Drop

Des mots de passe forts

Vous devez utiliser un mot de passe fort pour administrer votre site WordPress.
Un mot de passe fort comporte au minimum 12 caractères, en combinant des caractères alphanumériques et ASCII.
L'utilisation de lettres minuscules uniquement limite le nombre de caractères possibles à 26. Il est donc essentiel d'inclure des caractères alphanumériques, des lettres majuscules et des caractères ASCII courants afin d'augmenter le nombre de caractères nécessaires pour déchiffrer le mot de passe à 92.

Par exemple, voici les temps estimés pour déchiffrer un mot de passe à l'aide d'un processeur i5 à quatre cœurs :

- un mot de passe de 7 caractères prend 0,29 milliseconde. un mot de passe de 8 caractères prend 5 heures.
- Un mot de passe de 9 caractères prendra 4 mois à craquer.
- un mot de passe de 10 caractères mettra 1 décennie à être déchiffré
- un mot de passe de 12 caractères mettra 2 siècles à être déchiffré.

Pixel Drop

Authentification 2 facteurs

L'authentification à deux facteurs (2FA) ajoute une couche de sécurité très forte en demandant un code supplémentaire avec votre nom d'utilisateur et votre mot de passe d'administrateur WordPress afin de vous connecter à votre site web.

Différentes méthodes d'authentification à deux facteurs

- **Email** : vous recevrez le code par le biais d'une notification par email. Vous utiliserez le code envoyé dans votre boîte de réception comme code secondaire pour vous connecter.
- **Application mobile** : mot de passe à usage unique basé sur le temps sur votre appareil mobile à l'aide d'une application d'authentification à deux facteurs telle Google Authenticator.

La maintenance de Pixel Drop ajoute une authentification à deux facteurs à votre connexion d'administrateur WordPress et aux autres types d'utilisateurs qui se connectent à votre site. Vous pouvez choisir parmi plusieurs méthodes d'authentification à deux facteurs, y compris l'application mobile, l'email et les codes de récupération.

Pixel Drop

Sauvegardez votre site

Malheureusement, votre site peut être piraté même si vous suivez les meilleures pratiques de sécurité de WordPress. Si un pirate réussit à compromettre votre site, le fait de disposer d'une sauvegarde vous permettra de restaurer votre site dans un état totalement opérationnel.

WordPress n'ayant pas d'outil de sauvegarde intégré, une stratégie de sauvegarde solide est votre assurance en cas de problème.

L'utilisation d'un plugin de sauvegarde WordPress vous permet de sauvegarder facilement l'ensemble de votre site web. La maintenance de Pixel Drop permet de mettre en place des planifications de sauvegarde automatisées afin que les sauvegardes soient effectuées toutes les heures, tous les jours ou toutes les semaines. Vos fichiers de sauvegarde sont ensuite stockés dans une boîte sécurisée et décentralisée afin que vous puissiez y accéder en cas de panne de votre site web.

Pixel Drop

Checklist de sécurité

1. Limiter les tentatives de connexion
2. Utiliser des mots de passes forts
3. Authentifcation à deux facteurs
4. Mettez à jours votre site
5. Effectuez des sauvegardes régulières


pixel-drop.com
Pixel Drop