Le guide ultime pour la sécurisation des sites clients

KINSTA

Pour la version toujours à jour, scannez le
QR code ci-dessus ou allez sur:
https://kinsta.com/fr/ebooks/

Publié par Kinsta

Le guide ultime pour la sécurisation des sites clients

Table des matières

Le guide ultime pour la sécurisation des sites clients

Selon les statistiques en direct sur Internet, plus de 100 000 sites web sont piratés chaque jour. 😮 C'est pourquoi il est si important de prendre le temps de lire les recommandations ci-dessous pour mieux renforcer la sécurité de votre WordPress.

En matière de sécurité WordPress, il y a bien plus que le simple verrouillage de votre site, même si nous vous donnons ci-dessous les meilleures recommandations sur la manière de le faire.

Investir dans l'hébergement WordPress sécurisé

Commençons par la sécurité au niveau du serveur web, dont votre hébergeur WordPress est responsable. Il est très important que vous choisissiez un hébergeur en qui vous pouvez avoir confiance pour votre entreprise lorsque vous transférez les sites de vos clients chez eux.

Si vous hébergez WordPress sur votre propre VPS, vous devez avoir les connaissances techniques nécessaires pour faire ces choses vous-même. Mais pour être honnête, essayer d'être un administrateur système pour économiser 20 $ par mois n'est pas une façon efficace de gérer une entreprise.

Le durcissement des serveurs est la clé du maintien d'un environnement WordPress parfaitement sécurisé. Il faut plusieurs couches de mesures de sécurité au niveau matériel et logiciel pour garantir que l'infrastruc-

ture informatique qui héberge les sites WordPress est capable de se défendre contre des menaces sophistiquées, tant physiques que virtuelles.

C'est pourquoi les serveurs hébergeant WordPress doivent être mis à jour avec le système d'exploitation et les logiciels (de sécurité) les plus récents, ainsi que testés et analysés de manière approfondie pour détecter les vulnérabilités et les malwares.

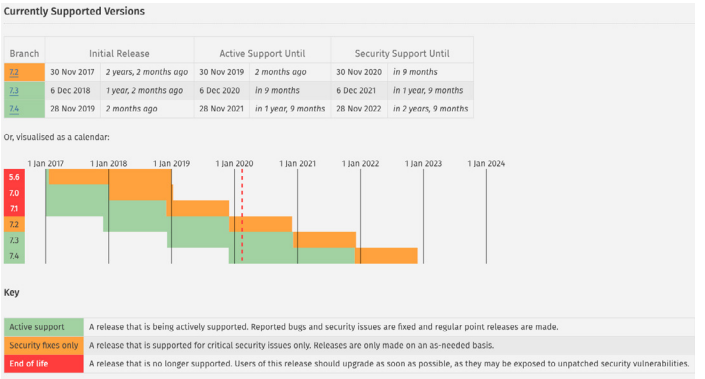
Des pare-feu au niveau du serveur et des systèmes de détection des intrusions doivent également être en place pour que les sites de vos clients soient bien protégés, même pendant les phases d'installation de WordPress et de construction du site web. Toutefois, tous les logiciels installés sur la machine, destinés à protéger le contenu de WordPress doivent être compatibles avec les derniers systèmes de gestion de bases de données pour maintenir des performances optimales. Le serveur doit également être configuré pour utiliser des réseaux sécurisés et des protocoles de cryptage de transfert de fichiers (tels que SFTP au lieu de FTP) afin de cacher les contenus sensibles aux intrus malveillants.

Chez Kinsta, nous utilisons la plateforme Google Cloud pour tous nos clients WordPress afin d'assurer un hébergement WordPress sécurisé. La sécurité est intégrée à notre architecture dès le début et c'est une méthode beaucoup plus sûre que les autres méthodes disponibles aujourd'hui.

Utilisez la dernière version de PHP

PHP est l'épine dorsale de tout site WordPress, il est donc très important de s'assurer que les sites de vos clients utilisent la dernière version sur votre serveur. Chaque version majeure de PHP est généralement entièrement prise en charge pendant deux ans après sa sortie.

Pendant cette période, les bugs et les problèmes de sécurité sont corrigés régulièrement. À partir d'aujourd'hui, toute personne utilisant la version PHP 7.1 ou une version inférieure n'a plus de support de sécurité et est exposée à des vulnérabilités de sécurité non corrigées.



Currently Supported Versions

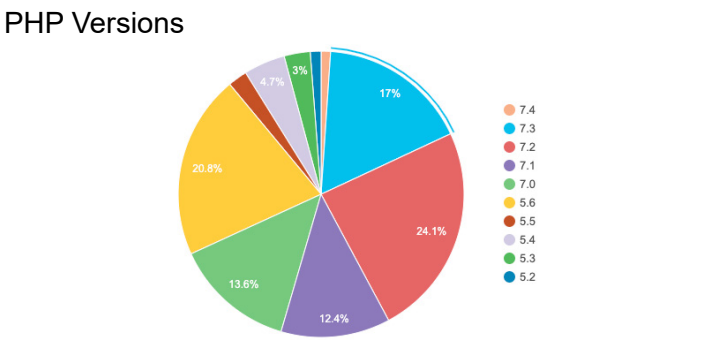
Branch	Initial Release		Active Support Until		Security Support Until	
7.2	30 Nov 2017	*2 years, 2 months ago*	30 Nov 2019	*2 months ago*	30 Nov 2020	*in 9 months*
7.3	6 Dec 2018	*1 year, 2 months ago*	6 Dec 2020	*in 9 months*	6 Dec 2021	*in 1 year, 9 months*
7.4	28 Nov 2019	*2 months ago*	28 Nov 2021	*in 1 year, 9 months*	28 Nov 2022	*in 2 years, 9 months*

Or, visualised as a calendar:

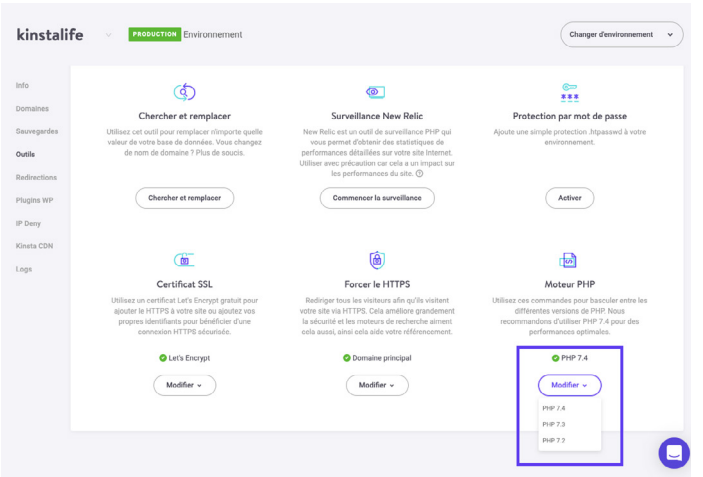
Key

Active support	A release that is being actively supported. Reported bugs and security issues are fixed and regular point releases are made.
Security fixes only	A release that is supported for critical security issues only. Releases are only made on an as-needed basis.
End of life	A release that is no longer supported. Users of this release should upgrade as soon as possible, as they may be exposed to unpatched security vulnerabilities.

Et devinez quoi? Selon la page officielle de WordPress Stats, environ 34% des utilisateurs de WordPress sont toujours en PHP 5.6 ou inférieur, ce qui signifie que plus d'un tiers des utilisateurs utilisent actuellement des versions de PHP qui ne sont plus prises en charge. C'est effrayant!



Chez Kinsta, nous ne recommandons que l'utilisation des versions stables et supportées de PHP, y compris les versions 7.2, 7.3 et 7.4. Les versions 5.6, 7.0 et 7.1 de PHP ont été supprimées progressivement. Vous pouvez même passer d'une version de PHP à l'autre en cliquant sur un bouton dans le tableau de bord de MyKinsta.



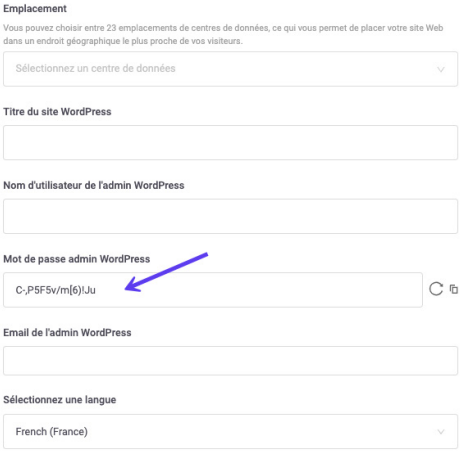
Si vous voulez l'essayer vous-même, rendez-vous sur demo.kinsta.com et essayez-le!

Utilisez des noms d'utilisateur et des mots de passe intelligents

Étonnamment, l'un des meilleurs moyens de renforcer la sécurité de WordPress consiste à utiliser des noms d'utilisateur et des mots de passe intelligents. Cela semble assez facile, non? Eh bien, consultez la liste annuelle 2019 de SplashData des mots de passe les plus populaires volés au cours de l'année (classés par ordre de popularité).

- 123456
- 123456789
- qwerty
- password
- 1234567
- 12345678
- 12345
- iloveyou
- 111111
- 123123

Le mot de passe le plus populaire est <<123456>>. C'est l'une des raisons pour lesquelles, ici chez Kinsta, sur les nouvelles installations de WordPress, nous forçons en fait un mot de passe complexe à être utilisé pour le login wp-admin de n'importe lequel de vos clients (comme on le voit ci-dessous sur notre processus d'installation en un clic). Ce n'est pas facultatif.



Découvrez cette fonctionnalité avec la démo de MyKinsta.

La fonction principale de WordPress wp_hash_password utilise le framework de hachage de mots de passe phpass et huit passes de hachage basé sur MD5. Et en ce qui concerne votre installation de WordPress, vous ne devez jamais utiliser le nom d'utilisateur <<admin>> par défaut sur les sites de vos clients, mais plutôt créer des noms d'utilisateur WordPress uniques pour leurs comptes d'administrateur.

Il est également important d'utiliser des mots de passe différents pour chaque site client. La meilleure façon de les stocker est de les stocker localement dans une base de données cryptée sur votre ordinateur.

Un bon outil gratuit pour cela est KeePass. Si vous ne voulez pas vous lancer dans cette voie, il existe également des gestionnaires de mots de passe en ligne tels que 1Password ou LastPass.

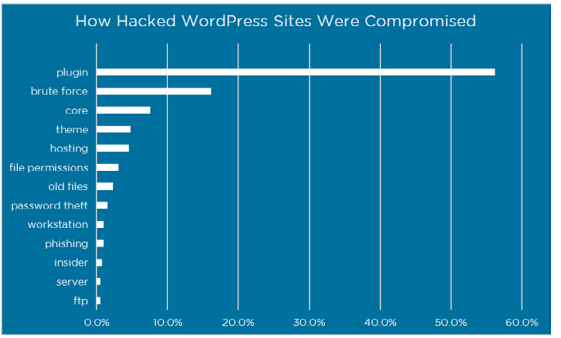
Utilisez toujours la dernière version de WordPress, des extensions et des thèmes

Un autre moyen très important de renforcer la sécurité des sites de vos clients est de les tenir toujours à jour. Cela inclut le noyau de WordPress, les extensions et les thèmes. Ces derniers sont mis à jour pour une bonne raison, et souvent ils comprennent des améliorations de la sécurité et des corrections de bugs.

Malheureusement, des millions d'entreprises utilisent des versions obsolètes de logiciels et d'extensions WordPress et pensent toujours être sur la bonne voie pour réussir. Elles citent des raisons pour lesquelles elles ne procèdent pas à la mise à jour, telles que <<leur site va se casser>> ou <<les modifications de base vont disparaître>> ou encore <<l'extension X ne fonctionnera pas>> ou <<elles n'ont tout simplement pas besoin de la nouvelle fonctionnalité>>.

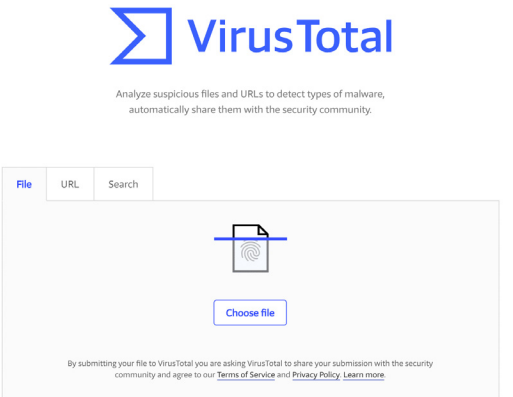
En fait, les sites web se cassent surtout à cause de bugs dans les anciennes versions de WordPress. Les modifications de base ne sont jamais recommandées par l'équipe WordPress et les développeurs experts qui comprennent les risques encourus. De plus, les mises à jour de WordPress comprennent principalement des correctifs de sécurité indispensables ainsi que les fonctionnalités supplémentaires requises pour faire fonctionner les dernières extensions.

Saviez-vous qu'il a été rapporté que les vulnérabilités d'extensions représentent 55,9% des points d'entrée connus des pirates informatiques ? C'est ce qu'a constaté WordFence dans une étude où ils ont interrogé plus de 1,000 propriétaires de sites WordPress qui avaient été victimes d'attaques. En mettant à jour vos extensions, vous pouvez mieux vous assurer que vous n'êtes pas l'une de ces victimes.



Il est également recommandé de n'installer que des extensions de confiance pour vos clients. Les catégories <<featured>> et <<popular>> du dépôt WordPress peuvent être un bon point de départ. Vous pouvez également les télécharger directement sur le site web des développeurs. Nous décourageons fortement toute utilisation d'extensions et de thèmes WordPress nulled.

Vous pouvez utiliser un outil en ligne comme VirusTotal pour analyser les fichiers d'une extension ou d'un thème afin de voir s'il détecte un type de malware.



Il existe également de nombreuses ressources pour vous aider à rester au courant des dernières mises à jour de sécurité et des vulnérabilités de WordPress. Vous en trouverez quelques-unes ci-dessous:

- AWP Security Bloggers: Une impressionnante ressource agrégée de plus de 20 flux de sécurité.
- CWPScan Vulnerability Database: Catalogue de plus de 10,000 vulnérabilités du coeur de WordPress, Extensions et Thèmes.

- ThreatPress: Base de données mise à jour quotidiennement des extensions et thèmes WordPress, ainsi que des vulnérabilités principales de WordPress..
- Archive officielle de sécurité WordPress

Verrouillez votre administration WordPress

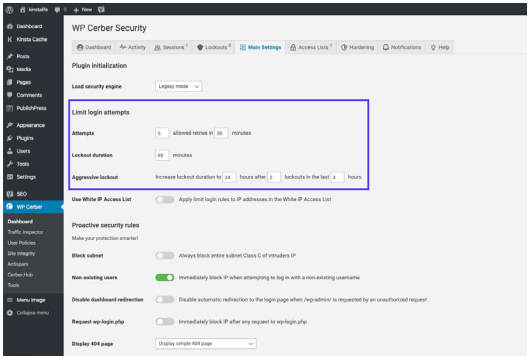
Parfois, la stratégie populaire de sécurité de WordPress par l'obscurité est suffisamment efficace pour une entreprise en ligne moyenne et un site WordPress. Si vous rendez plus difficile aux pirates de trouver certaines portes dérobées, vous avez moins de chances d'être attaqué. Le verrouillage de la zone d'administration WordPress de vos clients et de leur connexion est un bon moyen de renforcer votre sécurité. Deux bonnes façons d'y parvenir sont d'abord de changer votre URL de connexion wp-admin par défaut et aussi de limiter les tentatives de connexion.

Comment changer l'URL de votre connexion WordPress
Par défaut, l'URL de connexion de votre site WordPress est domaine.com/wp-admin. L'un des problèmes est que tous les robots, pirates et scripts le savent aussi. En changeant l'URL, vous pouvez faire de vous une moins bonne cible et mieux vous protéger contre les attaques par la force brute. Ce n'est pas une solution miracle, c'est simplement une petite astuce qui peut certainement vous aider à vous protéger.

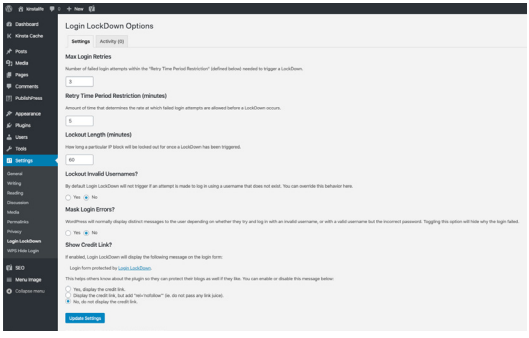
Pour changer votre URL de connexion WordPress, nous vous recommandons d'utiliser l'extension gratuite WPS Hide Login. N'oubliez pas de choisir un élément unique qui ne figure pas déjà dans une liste qu'un robot ou un script pourrait tenter de scanner.

Comment limiter les tentatives de connexion

Si la solution ci-dessus consistant à changer l'URL de connexion de votre administration peut contribuer à réduire la majorité des tentatives de connexion erronées, la mise en place d'une limite peut également être très efficace. L'extension gratuite Cerber Limit Login Attempts est un excellent moyen de configurer facilement les durées de verrouillage, les tentatives de connexion et les listes blanches et noires d'IPs.



Si vous recherchez une solution de sécurité WordPress plus simple, une autre excellente alternative est l'extension gratuite Login Lockdown.

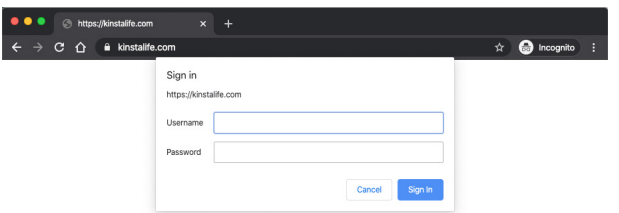


Login LockDown enregistre l'adresse IP et l'horodatage de chaque tentative de connexion échouée. Si plus d'un certain nombre de tentatives sont détectées dans une courte période de temps à partir de la même plage d'IP, la fonction de connexion est alors désactivée pour toutes les demandes de cette plage. Et il est totalement compatible avec l'extension WPS Hide Login que nous avons mentionnée ci-dessus.

Si vous déplacez le site de vos clients vers Kinsta, vous n'avez pas besoin d'installer d'extension supplémentaire pour les limites et notre plateforme bloque automatiquement les tentatives malveillantes.

Comment ajouter une authentification HTTP basique (protection htpasswd)

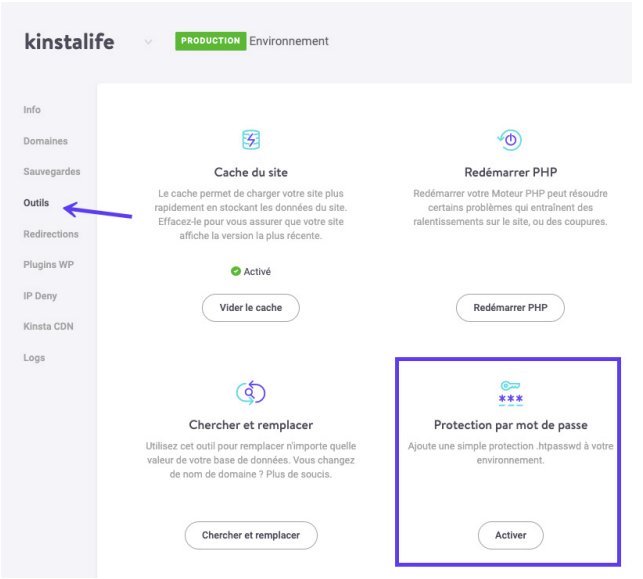
Une autre façon de verrouiller votre administration est d'ajouter une authentification HTTP. Cela nécessite un nom d'utilisateur et un mot de passe avant même de pouvoir accéder à la page de connexion de WordPress.



Découvrez cette fonctionnalité avec la démo de MyKinsta.

Important : il ne faut généralement pas l'utiliser sur les sites de eCommerce ou les sites d'adhésion. Mais cela peut être un moyen très efficace d'empêcher les robots de frapper votre site.

Si vous hébergez les sites de vos clients chez Kinsta, vous pouvez utiliser notre outil de protection facile par mot de passe (htpasswd) dans le tableau de bord de MyKinsta (voir en action sur le compte de démonstration gratuit de MyKinsta). Vous le trouverez dans la section <<Outils>> de votre site. Il suffit de cliquer sur <<Activer>>, de choisir un nom d'utilisateur et un mot de passe, et c'est parti!



Découvrez cette fonctionnalité avec la démo de MyKinsta.

Après son activation, chaque site WordPress demandera alors de vous authentifier pour y accéder. Vous pouvez modifier les identifiants à tout moment ou les désactiver lorsque vous n'en avez plus besoin.

Profitez de l'authentification à deux facteurs (2FA)

L'authentification à deux facteurs implique un processus en deux étapes dans lequel vous avez besoin non seulement de votre mot de passe pour vous connecter mais aussi d'une seconde méthode pour vous connecter. Dans la plupart des cas, cette méthode est efficace à 100 % pour prévenir les attaques par force brute sur les sites WordPress de vos clients.

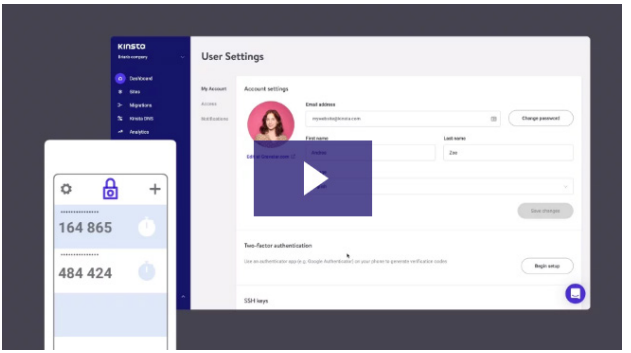
L'authentification à deux facteurs pour les sites clients comporte cependant deux volets.

Le premier est votre compte et/ou tableau de bord que vous avez chez votre hébergeur. Si quelqu'un y a accès, il peut modifier les mots de passe de tous vos clients, supprimer leurs sites web, modifier les enregistrements DNS et toutes sortes de choses horribles. Chez Kinsta, nous utilisons l'authentification 2FA pour votre tableau de bord MyKinsta parce que:

- La 2FA basée sur un authentificateur est plus sûre que la 2FA basée sur un SMS car elle n'est pas liée à votre numéro de téléphone portable et ne repose pas sur la technologie SMS existante. Cela rend la 2FA basée sur un authentificateur résistant aux techniques d'échange de cartes SIM.
- La 2FA basée sur un authentificateur peut être utilisée

avec des applications de gestion de mots de passe comme 1Password pour plus de commodité. En ajoutant les détails de votre 2FA à un gestionnaire de mots de passe, vous n'aurez pas besoin d'un périphérique externe pour vous connecter à MyKinsta.

Voici à quel point il est facile de l'activer:



La deuxième partie de l'authentification à deux facteurs concerne les installations WordPress réelles de vos clients. Pour cela, il existe quelques extensions que vous pouvez tester et recommander:

- Duo Two-Factor Authentication
- Google Authenticator
- Two Factor Authentication

Après avoir installé et configuré l'une des extensions ci-dessus sur un site client, ils disposent généralement d'un champ supplémentaire sur leur page de connexion WordPress pour entrer leur code de sécurité. Ou, avec l'extension Duo, ils se connecteront d'abord avec leurs identifiants et devront ensuite choisir une méthode d'authentification, comme Duo Push, call ou passcode.

Utiliser HTTPS pour les connexions cryptées - Certificat SSL

L'un des moyens les plus négligés pour renforcer la sécurité de WordPress est d'installer un certificat SSL et de faire fonctionner les sites par HTTPS. HTTPS (Hypertext Transfer Protocol Secure) est un mécanisme qui permet à tout navigateur ou application web de se connecter de manière sécurisée à un site web. Une grande idée fausse est que si les sites de vos clients n'acceptent pas les cartes de crédit, ils n'ont pas besoin de SSL.

Eh bien, expliquons quelques raisons pour lesquelles le HTTPS est important au-delà du simple eCommerce. De nombreux hébergeurs, dont Kinsta, offrent des certificats SSL gratuits avec Let's Encrypt.

6 raisons principales pour lesquelles le HTTPS est important au-delà du simple eCommerce

1. Sécurité supplémentaire
Quelle est l'importance des informations de connexion de vos clients ? Vous devez savoir qu'à chaque fois qu'un utilisateur se connecte, ces informations sont transmises au serveur en texte clair. Le HTTPS est absolument vital pour maintenir une connexion sécurisée entre un site web et un navigateur. Ainsi, vous pouvez mieux empêcher les pirates informatiques et/ou un intermédiaire d'accéder aux sites de vos clients..

2. SEO
Google a officiellement déclaré que le HTTPS est un facteur de classement. Comme la plupart de vos clients profiteraient probablement de tous les avantages possibles du SEO et des SERP pour battre leurs concurrents, c'est une évidence.

3. Confiance et crédibilité
Selon une enquête de GlobalSign, 28,9 % des visiteurs recherchent la barre d'adresse verte dans leur navigateur. Et 77 % d'entre eux craignent que leurs données soient interceptées ou utilisées à mauvais escient en ligne. En voyant ce cadenas vert, les clients auront instantanément l'esprit plus tranquille, sachant que leurs données sont plus sûres.

4. Données de référence
Beaucoup de gens ne se rendent pas compte que les données de référence HTTPS à HTTP sont bloquées dans Google Analytics. Qu'advient-il donc de ces données ? Eh bien, la plupart d'entre elles sont simplement regroupées avec la section <<trafic direct>>. Si quelqu'un passe de HTTP à HTTPS, le référent est quand même passé.

5. Avertissements sur Chrome
À partir du 24 juillet 2018, les versions de Chrome 68 et supérieures ont commencé à marquer tous les sites non-HTTPS comme <<Non sécurisé>> et, à partir de 2020, le navigateur populaire a commencé à diminuer la prise en charge des anciennes versions TLS. Google fait comprendre aux visiteurs qu'un site WordPress peut ne pas fonctionner sur une connexion sécurisée. C'est pourquoi le HTTPS est plus important que jamais!

6. Performance
Grâce à un protocole appelé HTTP/2, ceux qui utilisent des sites correctement optimisés par le biais du HTTPS peuvent souvent constater une amélioration de la vitesse. Le protocole HTTP/2 nécessite le HTTPS en raison de la prise en charge par les navigateurs. L'amélioration des performances est due à diverses raisons telles que la capacité de HTTP/2 à prendre en charge un meilleur multiplexage, le parallélisme, la compression HPACK avec codage Huffman, l'extension ALPN et le push serveur.

Et avec TLS 1.3, les connexions HTTPS sont encore plus rapides. Kinsta supporte TLS 1.3 sur tous nos serveurs et notre CDN Kinsta.

Consultez notre guide de migration HTTPS WordPress détaillé pour comprendre et en savoir plus dans notre comparaison TLS vs SSL.

Désactiver XML-RPC

Au cours des dernières années, le XML-RPC est devenu une cible de plus en plus importante pour les attaques par la force brute. Il existe quelques extensions WordPress comme Jetpack qui reposent sur le XML-RPC, mais la majorité des gens n'en ont pas besoin et il peut être avantageux d'en désactiver simplement l'accès.

Si vous êtes client chez Kinsta, vous n'avez pas à vous en inquiéter car nous avons mis en place des mesures actives et passives pour mettre fin aux attaques et aux intentions malveillantes. Plus précisément, lorsqu'une attaque via XML-RPC est détectée, un petit bout de code est ajouté dans le fichier de configuration Nginx pour les bloquer et produire une erreur 403.

Ajouter les derniers en-têtes de sécurité HTTP

Une autre mesure que vous pouvez prendre pour renforcer la sécurité de votre site client WordPress est de tirer parti des en-têtes de sécurité HTTP. Ceux-ci sont généralement configurés au niveau du serveur web et indiquent au navigateur comment se comporter lors de la manipulation du contenu de vos sites clients. Il existe de nombreux en-têtes de sécurité HTTP différents, mais les plus importants sont généralement ceux qui se trouvent ci-dessous.

- Content-Security Policy
- X-XSS-Protection
- Strict-Transport-Security
- X-Frame-Options
- Public-Key-Pins
- X-Content-Type

Vous pouvez vérifier quels en-têtes sont actuellement activés sur chaque installation de WordPress en lançant les Outils de développement Chrome et en regardant l'en-tête de la réponse initiale de votre site.

Voici un exemple sur kinstalife.com (un site de démonstration). Vous pouvez voir que nous utilisons l'en-tête x-content-type-options.

En ce qui concerne les sites clients, comme dans l'exemple présenté, les options de type x-content sont toujours ajoutées par défaut, tandis que les options de type x-frame et Strict Transport Security ne sont définies que si elles sont nécessaires.

Si vous avez besoin de scanner les sites de vos clients, vous pouvez le faire avec l'outil gratuit securityheaders.io de Scott Helme.

Il est également important de se rappeler que lorsque vous implémentez des en-têtes de sécurité HTTP, comment cela peut affecter vos sous-domaines WordPress. Par exemple, si vous ajoutez l'en-tête Content Security Policy et que vous limitez l'accès par domaines, vous devez alors ajouter vos propres sous-domaines également. Si vous ne savez pas comment les mettre en place, vous pouvez toujours demander à votre hébergeur s'il peut vous aider.

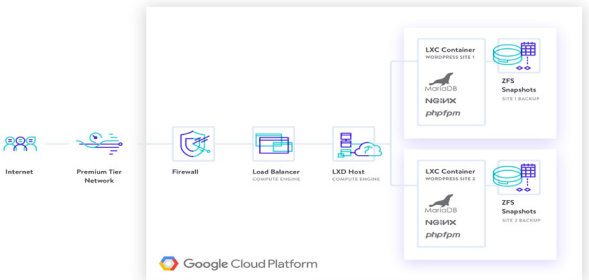
Utiliser les extensions de sécurité WordPress

Il existe un grand nombre de développeurs et d'entreprises qui proposent d'excellentes solutions pour vous aider à mieux protéger votre site WordPress. Parmi les plus remarquables, citons:

- Sucuri Security
- iThemes Security
- Wordfence Security
- WP Security Audit Log
- WP fail2ban
- All In One WP Security & Firewall
- SecuPress
- BulletProof Security

- VaultPress
- Google Authenticator – Two Factor Authentication
- Security Ninja
- Defender
- Astra Web Security
- Shield Security
- Hide my WP
- WebARX

Kinsta dispose de pare-feu matériels, d'une sécurité active et passive, de contrôles de disponibilité à la minute près et de nombreuses autres fonctionnalités avancées pour empêcher les pirates d'accéder à vos données. Si, malgré tous nos efforts, votre site est compromis, nous le réparerons gratuitement.

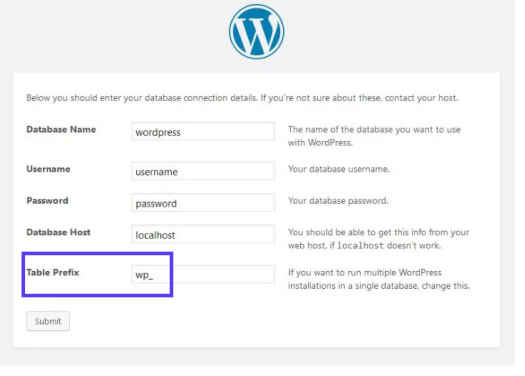


Une fonctionnalité très importante que de nombreuses extensions de sécurité comprennent est un utilitaire de somme de checksum. Cela signifie qu'ils inspectent chacune des installations WordPress de votre client et recherchent les modifications apportées aux fichiers de base tels que fournis par WordPress.org (via l'API). Tout changement ou modification de ces fichiers pourrait indiquer un piratage.

Vous pouvez également utiliser WP-CLI pour effectuer votre propre vérification. Consultez ces extensions de sécurité supplémentaires de WordPress qui peuvent vous aider à bloquer les méchants.

Renforcer la sécurité des bases de données

Il existe plusieurs façons d'améliorer la sécurité de votre base de données WordPress. La première consiste à utiliser un nom de base de données intelligent. En changeant le nom de votre base de données pour un nom plus obscur, vous contribuez à protéger leur site en rendant plus difficile l'identification et l'accès des pirates informatiques aux détails de votre base de données.

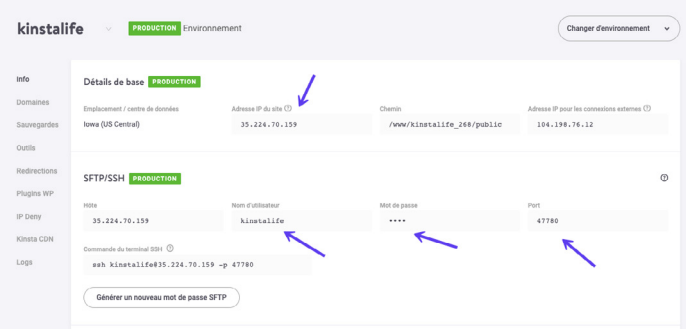


Une deuxième recommandation consiste à utiliser un préfixe de table de base de données différent. Lorsque vous installez WordPress, il vous demande un préfixe de table. Par défaut, WordPress utilise wp_. Changer ce préfixe pour quelque chose comme 39xw_ peut être beaucoup plus sûr.

Si vous êtes un client de Kinsta et que vous hébergez tous les sites de vos clients chez nous, ce n'est pas nécessaire. Nous avons verrouillé le site et la base de données pour vous!

Toujours utiliser des connexions sécurisées

On ne saurait trop insister sur l'importance d'utiliser des connexions sécurisées ! Assurez-vous que votre hébergeur WordPress prend des précautions telles que proposer SFTP ou SSH. SFTP ou Secure File Transfer Protocol (également connu sous le nom de protocole de transfert de fichiers SSH), est un protocole réseau utilisé pour les transferts de fichiers. Il s'agit d'une méthode plus sûre que le FTP standard.



Découvrez cette fonctionnalité avec la démo de MyKinsta.

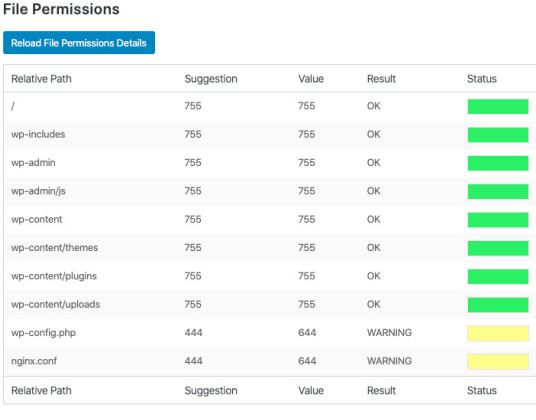
Chez Kinsta, nous ne prenons en charge que les connexions SFTP afin de garantir que vos données restent sûres et cryptées. La

plupart des hébergeurs WordPress utilisent aussi généralement le port 22 pour le SFTP. Nous allons un peu plus loin ici chez Kinsta et chaque site a un port aléatoire qui peut être trouvé dans votre tableau de bord MyKinsta.

Vérifier les autorisations de fichiers et de serveurs

Les autorisations de fichiers sur les installations de vos clients et les serveurs web sont essentielles pour renforcer la sécurité de ces environnements. Si les autorisations sont trop souples, quelqu'un pourrait facilement accéder à leur site et faire des ravages. D'un autre côté, si vos autorisations sont trop strictes, cela pourrait casser les fonctionnalités de leur site. Il est donc important de définir les bonnes autorisations de manière générale.

Vous pouvez utiliser une extension gratuite comme iThemes Security pour scanner les autorisations sur les sites WordPress de vos clients.


File Permissions

Reload File Permissions Details

Relative Path	Suggestion	Value	Result	Status
/	755	755	OK	
wp-includes	755	755	OK	
wp-admin	755	755	OK	
wp-admin/js	755	755	OK	
wp-content	755	755	OK	
wp-content/themes	755	755	OK	
wp-content/plugins	755	755	OK	
wp-content/uploads	755	755	OK	
wp-config.php	444	644	WARNING	
nginx.conf	444	644	WARNING	
Relative Path	Suggestion	Value	Result	Status

Voici quelques recommandations typiques concernant les autorisations de fichiers et de dossiers dans WordPress:

- Tous les fichiers doivent être en 644 ou 640. Exception : wp-config.php doit être réglé en 440 ou 400 pour empêcher les autres utilisateurs du serveur de le lire.
- Tous les dossiers doivent être en 755 ou 750.
- Il ne faut jamais mettre 777 aux dossiers, même pour le dossier uploads.

Voir l'article du Codex WordPress sur la modification des autorisations de fichiers pour une explication plus approfondie.

Protection contre les DDoS

La DDoS est un type d'attaque DOS où plusieurs systèmes sont utilisés pour cibler un seul système, ce qui provoque une attaque par déni de service (DoS). Les attaques DDoS ne sont pas nouvelles - selon Britannica, le premier cas documenté remonte au début de l'année 2000. Contrairement aux pirates informatiques, ces types d'attaques ne nuisent généralement pas à votre site, mais le rendent simplement inaccessible pendant quelques heures ou quelques jours.

Que pouvez-vous faire pour vous protéger ? L'une des meilleures recommandations est de faire appel à un service de sécurité tiers réputé comme Cloudflare ou Sucuri.

Leur protection DDoS avancée peut être utilisée pour atténuer les attaques DDoS de toutes formes et de toutes tailles, y compris celles qui visent les protocoles UDP et ICMP, ainsi que les attaques

SYN/ACK, l'amplification DNS et la couche 7. Parmi les autres avantages, on peut citer le fait de vous placer derrière un proxy qui permet de masquer votre adresse IP d'origine, bien que ce ne soit pas à l'épreuve des balles.

Ne négligez pas le fournisseur que votre hébergeur utilise, car c'est aussi assez important.

Des pare-feu matériels, tels que le pare-feu de la plateforme Google Cloud que nous utilisons chez Kinsta, sont en place et ont des restrictions très strictes basées sur les logiciels pour protéger les sites de vos clients et ont également des logiciels en place pour détecter les attaques DDoS lorsqu'elles se produisent.

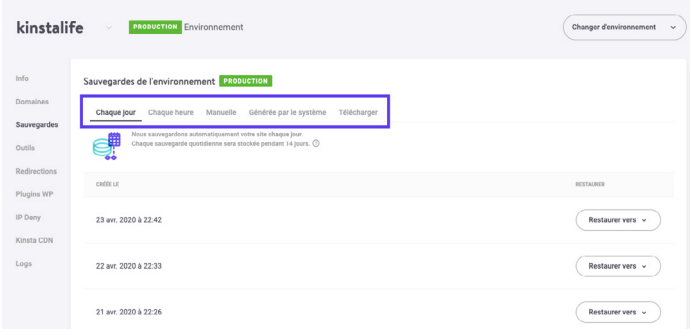
Cela signifie que vous et vos clients bénéficiez d'un modèle de sécurité qui a été développé au cours des 15 dernières années et qui sécurise actuellement des produits et services tels que Gmail, Search, etc. Google emploie actuellement plus de 500 professionnels de la sécurité à temps plein.

En plus de la plateforme Google Cloud, nous utilisons également des conteneurs Linux (LXC et LXD) pour les orchestrer, ce qui nous permet d'isoler complètement non seulement chaque compte, mais aussi chaque site WordPress distinct. Malgré cela vous avez des soucis? Kinsta propose des services gratuits de réparation de hack et de suppression de malwares. Si le site d'un de vos clients est infecté, notre équipe de support fera tout ce qu'il faut pour le nettoyer.

Obtenez plus de détails sur le sérieux avec lequel nous prenons la sécurité chez Kinsta!

Prenez toujours des copies de sauvegarde

Quel que soit le degré de sécurité de votre site, il ne sera jamais sûr à 100 %. C'est pourquoi vous voulez des sauvegardes au cas où le pire arriverait. Les sauvegardes sont la seule chose dont tout le monde sait qu'il a besoin, mais qu'il ne prend pas toujours. La plupart des recommandations présentées ici sont des mesures de sécurité que vous pouvez prendre pour mieux protéger les sites de vos clients et votre entreprise.



Découvrez cette fonctionnalité avec la démo de MyKinsta.

La plupart des fournisseurs d'hébergement WordPress infogéré fournissent désormais des sauvegardes. Kinsta dispose de cinq types de sauvegardes différents:

- Quotidiennement : Kinsta crée des sauvegardes automatisées de tous les sites de vos clients toutes les 24 heures afin que vous puissiez vous reposer en toute tranquillité la nuit.

- Toutes les heures: Si vous avez besoin d'un calendrier de sauvegarde plus fréquent, vous pouvez activer des sauvegardes automatiques de 6 heures ou d'une heure pour tout site cible qui en a besoin (cela vient en plus de votre plan mensuel).
- Manuelles: si les sauvegardes automatiques ne suffisent pas, vous pouvez créer des sauvegardes manuelles pour chaque site que vous gérez et disposer de cette copie supplémentaire pendant 14 jours ou plus, en fonction de votre plan actuel.
- Générées par le système: avant les tâches critiques telles que l'utilisation de l'outil de recherche-remplacement dans MyKinsta, le passage d'un environnement de staging en production et la restauration d'une sauvegarde dans votre environnement en production, Kinsta déclenchera des sauvegardes générées par le système.
- Archives téléchargeables: si tout cela ne suffit pas, une fois par semaine, vous pouvez télécharger un fichier zip de chaque site client contenant les fichiers du site et un fichier SQL contenant le contenu de la base de données du site.

Les options de sauvegarde ne viennent pas seules, car Kinsta vous permet de restaurer facilement n'importe quel site en un seul clic. C'est pratique, n'est-ce pas?

Testez gratuitement à quel point c'est facile de créer une sauvegarde avec MyKinsta!

Si votre hébergeur ne dispose pas de sauvegardes, il existe des extensions WordPress très répandues que vous pouvez utiliser pour automatiser le processus.

Extensions de sauvegarde WordPress

Les extensions de sauvegarde WordPress vous permettent de récupérer vos sauvegardes via FTP ou de les intégrer à une source de stockage externe telle qu'Amazon S3, Google Cloud Storage, Google Drive ou Dropbox. Nous vous recommandons vivement d'opter pour une solution incrémentale afin d'utiliser moins de ressources:

- Duplicator
- WP Time Capsule
- BackupBuddy
- UpdraftPlus
- BackUpWordPress
- BackWPup
- WP BackItUp

Kinsta n'autorise pas les extensions de sauvegarde non incrémentales pour des raisons de performances : nous gérons tout cela pour vous au niveau du serveur afin que cela ne ralentisse pas les sites de vos clients.

Résumé

La sécurité est un jeu de couches. Plus vous réussissez à superposer de nouvelles couches de sécurité, plus les sites de vos clients

seront sécurisés. Tout commence par l'utilisation de mots de passe intelligents, la mise à jour du coeur et des extensions, et le respect des autres bonnes pratiques de sécurité dont nous avons parlé ici.

Mais ce n'est pas tout ce que vous devez faire pour réduire vos chances d'avoir à faire face à des sites clients piratés. En choisissant un hébergeur WordPress infogéré comme Kinsta, la plupart des mesures de sécurité sont prises en charge pour vous, ce qui vous permet de construire une base solide, sûre et évolutive pour assurer l'avenir des sites de vos clients. Et celui de votre entreprise.

Vous voulez essayer la facilité de gestion des sites clients sur Kinsta?

Rendez-vous sur demo.mykinsta.com!


KINSTA