

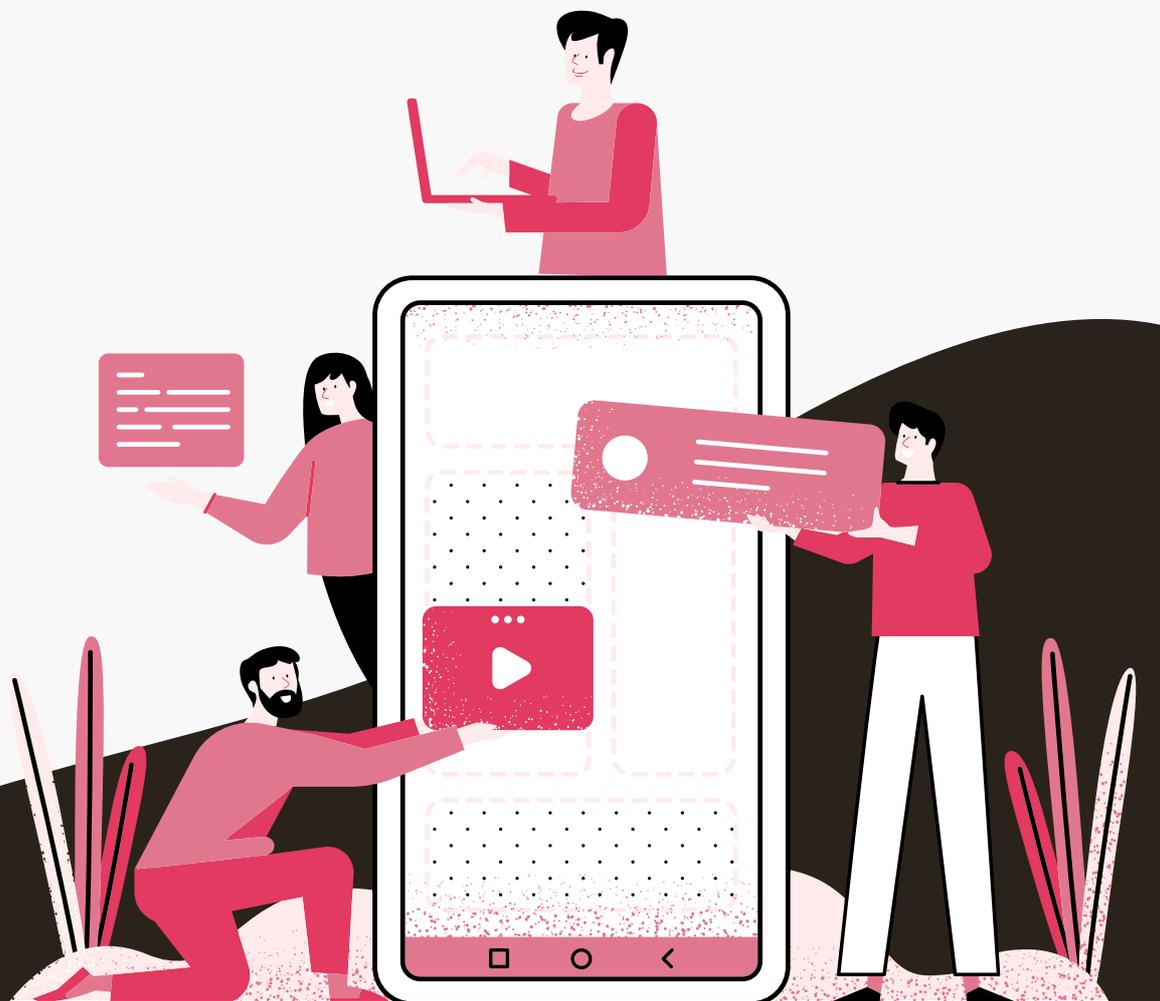
Hack serveur

Pour Eclolink.

FAIT PAR

Kevin JANIKY

FÉVRIER 2024



Analyse

- Réapparition fréquente des **hacks** malgré un nettoyage initial.
- Découverte de logiciels non installés par nous sur le serveur, notamment un **sniffer de données**, un **antivirus inadéquat** pour un serveur, et un logiciel ajoutant constamment des **fichiers hackés**.
- **Mises à jour manquantes** des logiciels et des applications, entraînant des failles de sécurité sur les plugins de WordPress.
- Coexistence de **deux versions de PHP** sur le serveur, entraînant des problèmes d'isolation et de configuration lors de la modification de la configuration PHP.
- **Corruption** du **sitemap** due à une **injection de code**.
- **Exposition** des **mots de passe** dans des fichiers **accessibles**.
- **Compromission** des **bases de données** avec une possible **fuite de données**, associée à la découverte d'un plugin pour lire la base de données.
- Présence d'un **mini-shell public** permettant un **accès au serveur** via remote SSH pour **n'importe quel utilisateur**.



Resultat du hack

- **Sitemap corrompue** contenant des dizaines de milliers d'URL externes - **SEO impacté**.
- **Suppression du contenu** média.
- Référentiel **Git** partiellement **supprimé**, par exemple, celui de "Briottet".
- **Corruption** partielle des **sauvegardes**.
- **Surcharge** fréquente du **serveur**, atteignant régulièrement **90%** d'utilisation lorsque les logiciels malveillants sont activés.
- **Infection complète** de **WordPress**.
- **Exposition** de la **base de données**, avec un risque potentiel de **fuite de données**.
- **Exposition** et risque potentiel de **fuite des tokens**.



WPScan

- J'ai effectué des analyses en utilisant **WPScan**.
- Une société américaine reconnue pour la sécurité de WordPress.
- J'ai également pris un rendez-vous avec eux pour obtenir une proposition commerciale.
- En résumé, WPScan détecte les failles CVE (Common Vulnerabilities and Exposures) et les signales.
- Pour moi l'offre n'est pas abordable dans la situation actuelle.

WordPress' open-source platform powers over 43% of the internet, making it a lucrative target for hackers

90% of all hacking attempts on CMS' are WordPress attacks

There are close to 90,000 attacks per minute on WordPress

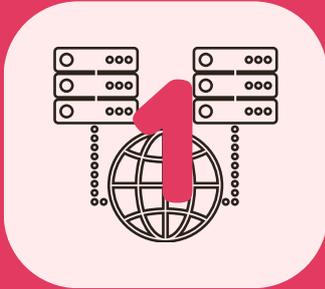
A hacking attempt is made once every 20 minutes on the average WordPress site

52% of all WordPress vulnerabilities are caused by out-of-date plugins

The screenshot shows a pricing table with three columns representing different terms: 12-month term, 36-month term (Recommended), and 24-month term. Each column displays a price, a 'Select' button, and a payment method indicator.

Term	Price	Discount	Payment Method
12-month term	\$10,000.00 / year		✓ Paid annually
36-month term (Recommended)	\$20,100.00	33% OFF (from \$30,000.00)	✓ Paid in full in advance
24-month term	\$16,000.00	20% OFF (from \$20,000.00)	✓ Paid in full in advance

Proposition



Isolation des sites à risque :

- Isolation de Briottet sur un serveur dédié.
- Isolation des autres VIP sur un serveur dédié.
- Nettoyage des sites infectés.



Nettoyage du serveur actuel :

- Mise en place d'un nouveau serveur avec PHP 7.4 en raison du nombre élevé de sites dans cette version.
- Nettoyage des sites infectés.
- Isolation de chaque site dans un environnement semi-cloisonné pour une sécurité renforcée en cas de piratage.
- Remise en place du système de sauvegardes
- Ajout du système de sauvegardes sur les nouveaux serveurs.
- Isolation des préprods sur un serveur dédié.



Phase de Maintenance & surveillance :

- Déploiement des nouveaux sites dans des environnements isolés, avec la possibilité pour le client de déployer les sites lui-même, mais une configuration ultérieure devra être effectuée.
- Mises à jour régulières des 4 serveurs.
- Pentest régulier des sites (spécifique à WordPress).
- Détecteur de sites WordPress non mis à jour avec un rapport mensuel pour la liste des sites à mettre à jour.
- Log monitoring / Observability - AtomikAgency
- Malware scan. - AtomikAgency
- Sitemap Checker - AtomikAgency
- File edited detector - AtomikAgency

Informations

- La proposition ne prend pas en compte la mise à jour des sites WordPress car cela dépend de l'état de chaque site. Si une mise à jour est simple, le client peut la faire rapidement. Cependant, si les sites sont obsolètes, des développements supplémentaires pourraient être nécessaires pour les mettre à jour en toute sécurité.

Les mesures proposées dans la proposition ne peuvent garantir une isolation totale à 100% pour plusieurs raisons :

- Les technologies envisagées peuvent rendre difficile l'atteinte d'un niveau de sécurité optimal.
- La sécurité exige une vigilance constante, aussi bien pendant la phase de développement que lors de l'exploitation.
- Les limitations budgétaires peuvent restreindre la mise en place d'une infrastructure plus robuste.
- La volonté de maintenir un contrôle sur les déploiements peut empêcher l'adoption des dernières technologies de sécurité.
- Rien n'est jamais totalement sûr en matière de sécurité informatique.

L'isolation dans cette proposition comprend :

- Séparation des utilisateurs d'exécution pour éviter l'accès non autorisé entre sites.
- Isolation de FPM pour exécuter les scripts PHP de manière indépendante.
- Gestion des droits pour contrôler l'accès aux fichiers et aux répertoires.
- Désactivation de certaines fonctions PHP inutiles pour réduire les risques.

Ces mesures renforcent la sécurité en évitant la propagation d'attaques et en réduisant les zones d'exposition.

Budget

- Le prix total pour la phase 1 et 2 sera de 4000 € hors taxes
- Le coût de la phase 3 s'élève à 840 € hors taxes mensuel, représentant trois jours de travail.

Budget Serveur

5 Serveurs :

Briottet

CAX21	vCPU 4 Ampere	RAM 8 GB	Disk space 80 GB	Traffic 20 TB	IPv4 ✓	Locations 🇩🇪 +	€ 0.0120 / hr	€ 7.72 / mtl.
-------	-------------------------	-------------	---------------------	------------------	-----------	-------------------	---------------	---------------

VIP

CAX31	vCPU 8 Ampere	RAM 16 GB	Disk space 160 GB	Traffic 20 TB	IPv4 ✓	Locations 🇩🇪 +	€ 0.0240 / hr	€ 14.86 / mtl.
-------	-------------------------	--------------	----------------------	------------------	-----------	-------------------	---------------	----------------

Php 7.4

CAX31	vCPU 8 Ampere	RAM 16 GB	Disk space 160 GB	Traffic 20 TB	IPv4 ✓	Locations 🇩🇪 +	€ 0.0240 / hr	€ 14.86 / mtl.
-------	-------------------------	--------------	----------------------	------------------	-----------	-------------------	---------------	----------------

Php 7.3

CAX31	vCPU 8 Ampere	RAM 16 GB	Disk space 160 GB	Traffic 20 TB	IPv4 ✓	Locations 🇩🇪 +	€ 0.0240 / hr	€ 14.86 / mtl.
-------	-------------------------	--------------	----------------------	------------------	-----------	-------------------	---------------	----------------

Preprod

CPX21	vCPU 3 AMD	RAM 4 GB	Disk space 80 GB	Traffic 20 TB	IPv4 ✓	Locations 🇩🇪 + 🇺🇸	€ 0.0143 / hr	€ 8.98 / mtl.
-------	----------------------	-------------	---------------------	------------------	-----------	----------------------	---------------	---------------

70€ > ~60€

Divers

Google cloud

143,62€ > ~40€ / ~60€

