Plan d'Améliorations du Système d'Information

Site: Site: https://env-9206928-wp02-nosecure.hidora.com/

Introduction

Le présent plan d'améliorations a pour objectif d'optimiser les performances, renforcer la sécurité et accroître la scalabilité du Système d'Information (SI). Les recommandations abordent des domaines clés tels que la gestion des cookies, la sécurisation de l'infrastructure, l'amélioration des performances en temps réel, et l'optimisation des processus internes. Ces améliorations sont basées sur une analyse approfondie des vulnérabilités et des points faibles du système actuel, avec un accent particulier sur les meilleures pratiques en matière de sécurité et de performance.

Améliorations de la Performance

1.1. Mettre en place des outils de surveillance

L'intégration d'un système de Real User Monitoring (RUM) permettra de suivre les performances du site en temps réel, en analysant l'expérience utilisateur directement sur les appareils des visiteurs. Cela permettra de mieux comprendre les points de friction dans l'interface et d'optimiser la vitesse de chargement des pages.

Action recommandée:

- Installer des outils comme Pingdom pour monitorer les performances en temps réel.
- Analyser les données récoltées pour identifier les goulets d'étranglement et optimiser la vitesse de chargement des pages.

1.2. Optimiser le Système de Cache

Actuellement, le site utilise W3 Total Cache, mais la version obsolète présente des risques de sécurité. Mettre à jour ce plugin ou le remplacer par une solution plus moderne assurera une mise en cache plus efficace.

Action recommandée:

Mettre à jour W3 Total Cache ou envisager son remplacement par des solutions comme WP Rocket ou LiteSpeed Cache, qui sont mieux maintenues et plus sécurisées.

1.3. Optimisation de WP-Cron

Le système WP-Cron peut être responsable de charges inutiles sur le serveur. Il est recommandé de le configurer pour qu'il fonctionne de manière externe via un cron job afin de minimiser son impact sur les performances.

Action recommandée:

Configurer WP-Cron pour s'exécuter via un cron job externe ou le désactiver si ce n'est pas nécessaire.

2. Améliorations de la Sécurité

2.1. Mettre à jour les Composants WordPress et Plugins

La mise à jour régulière des composants WordPress (version 6.6.2) et des plugins (notamment W3 Total Cache) est essentielle pour garantir la sécurité du site.

Action recommandée:

- Mettre à jour WordPress, le thème, et les plugins vers leurs dernières versions stables.
- Vérifier que tous les plugins sont maintenus et remplacer ceux qui ne le sont pas par des alternatives plus sécurisées.

2.2. Désactivation de XML-RPC

Le XML-RPC est souvent utilisé pour des attaques par force brute et des attaques DDoS. Il est donc recommandé de le désactiver si cette fonctionnalité n’est pas utilisée.

Action recommandée:

Désactiver XML-RPC dans le fichier .htaccess ou via un plugin de sécurité si cette fonctionnalité n'est pas nécessaire.

2.3. Sécurisation des Fichiers Sensibles

Le fichier wp-config.php contient des informations sensibles et doit être sécurisé. Vérifier les permissions des fichiers sensibles et de limiter leur accès.

Action recommandée:

- Vérifier et modifier les permissions des fichiers sensibles pour qu'ils ne soient accessibles qu’aux utilisateurs autorisés.
- Ajouter des règles de sécurité dans le fichier .htaccess pour protéger les fichiers importants.

2.4. Implémentation de l'Authentification Multifactorielle (MFA)

L’activation de l'authentification multifactorielle (MFA) pour tous les comptes administratifs du site permettra de rédu

Action recommandée:

Configurer la MFA via des plugins comme Google Authenticator ou Authy.

2.5. Configuration d'un WAF (Web Application Firewall)

L'utilisation d'un pare-feu d'application web (WAF) est essentielle pour protéger le site contre les attaques malveillantes courantes comme les SQL injections, les XSS et les DDoS.

Action recommandée:

Installer un WAF comme Cloudflare ou ModSecurity pour renforcer la sécurité du site.

2.6. Surveillance des Vulnérabilités

Il est important de surveiller activement les vulnérabilités potentielles du site pour pouvoir réagir rapidement aux nouvelles menaces.

Action recommandée:

- Utiliser des outils comme WPScan pour scanner régulièrement le site à la recherche de vulnérabilités.
- Mettre en place des alertes pour toute détection de nouvelles vulnérabilités.

3. Améliorations de la Scalabilité

3.1. Renforcer la Gestion des Cookies et la Conformité RGPD

La gestion des cookies et la conformité au RGPD sont essentielles pour garantir que le site respecte les lois sur la protection des données.

Action recommandée:

- Mettre à jour la bannière de consentement aux cookies pour inclure des options de personnalisation des cookies.
- Utiliser des outils comme OneTrust ou Cookiebot pour faciliter la gestion des cookies et la conformité au RGPD.

3.3. Surveillance de la Scalabilité du Serveur

Une surveillance continue de l'infrastructure serveur permettra de détecter les goulets d'étranglement et d’assurer que le site peut évoluer efficacement en fonction du volume de trafic.

Action recommandée: Utiliser des outils comme ELK ou Promotheus et grafana, ou AWS CloudWatch pour surveiller la charge du serveur et ajuster les ressources en conséquence.

Conclusion

Les recommandations proposées visent à améliorer la performance, la sécurité, et la scalabilité du Système d'Information. La mise en œuvre de ces actions contribuera à réduire les vulnérabilités existantes, améliorer l'expérience utilisateur, et garantir la conformité aux normes de sécurité et de confidentialité. Une surveillance continue et des mises à jour régulières des composants du système sont essentielles pour maintenir un environnement sécurisé et performant.