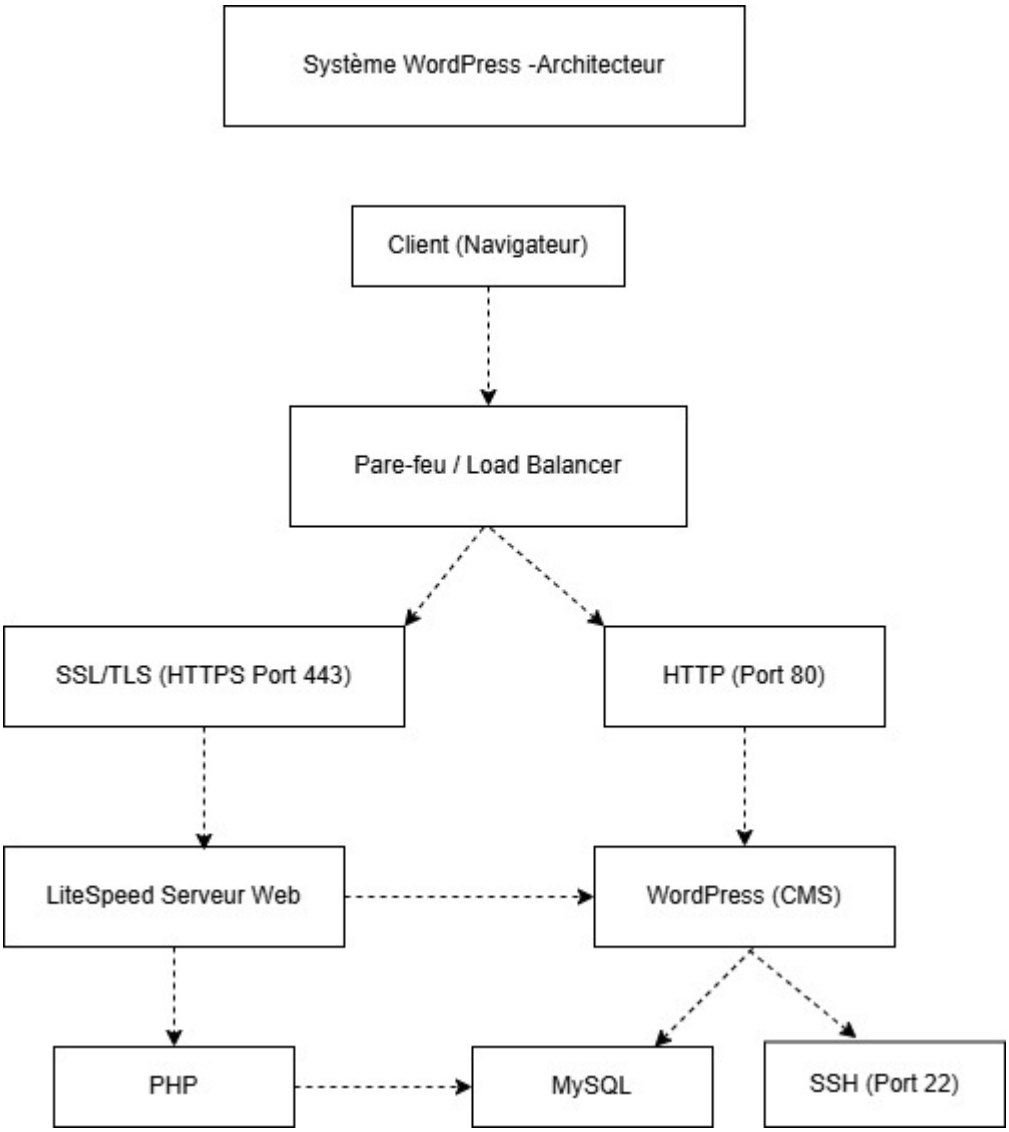
Rapport d'analyse détaillé

Site: https://env-8796793-wp02-ter.hidora.com

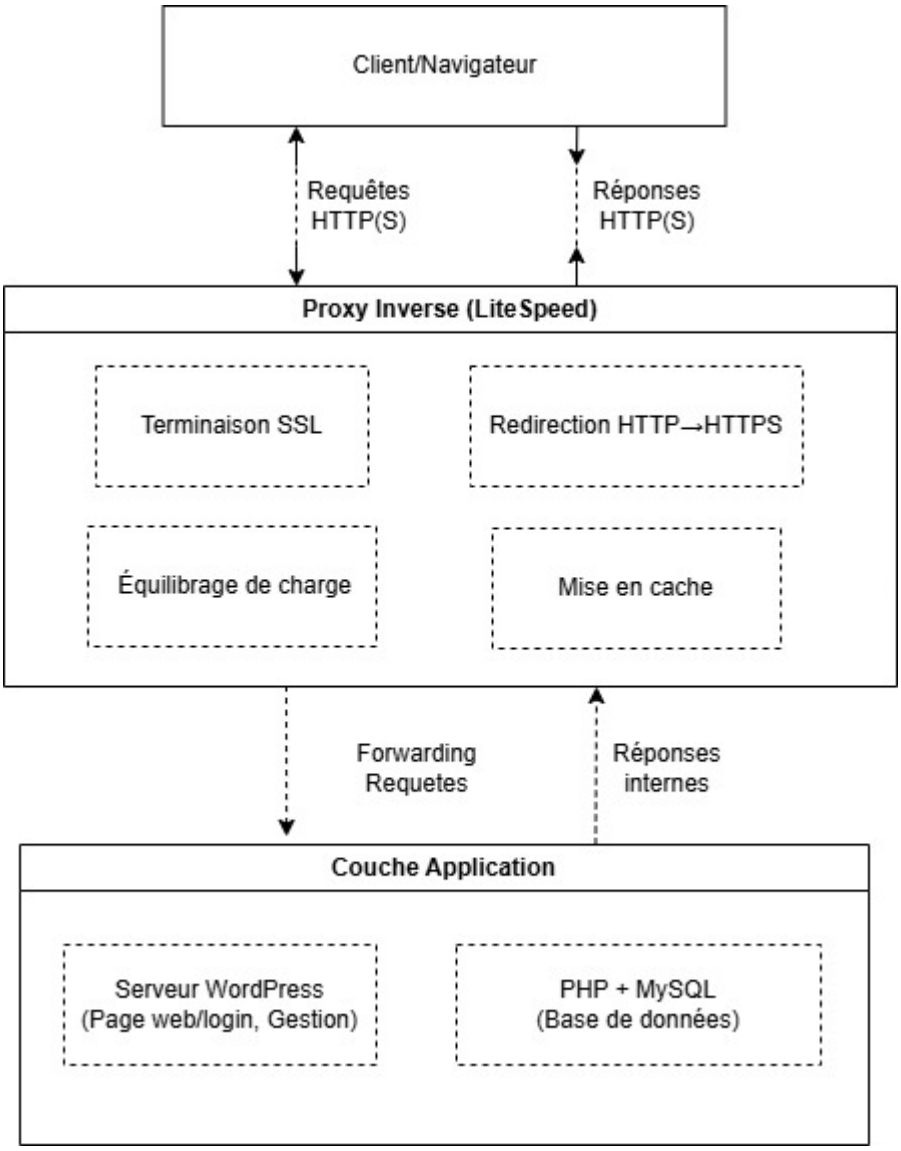
Introduction

Ce rapport présente les résultats d'un audit de sécurité réalisé sur le système d'information du site web env-8796793-wp02.hidora.com. L'objectif de cet audit est d'évaluer la sécurité du système, d'identifier les vulnérabilités et les risques potentiels, et de fournir des recommandations pour améliorer la sécurité et la résilience du système d'information. L'audit couvre les aspects de performance, de sécurité, de disponiblité gestion des données.

Architecture du Système



Flux d'Informations



Résultats de l'Audit de Sécurité

L'audit de sécurité a été effectué sur plusieurs niveaux de l'architecture du système d'information. Voici les points principaux identifiés lors de l'audit :

Points Forts

- Serveur Web performant (LiteSpeed): Le serveur est bien optimisé pour gérer des connexions simultanées, notamment avec un cache intégré, idéal pour des sites comme WordPress.

- Sécurisation via HTTPS et HSTS: Le site utilise des connexions HTTPS sécurisées et applique HTTP Strict Transport Security (HSTS), garantissant une communication sécurisée entre le client et le serveur.

- Accès SSH sécurisé: Le serveur est configuré pour accepter uniquement des connexions SSH par clés publiques, augmentant la sécurité par rapport aux connexions par mot de passe.

- HTTP/3 activé: Le support du protocole HTTP/3 améliore la performance de la connexion et la gestion de la latence, notamment pour les utilisateurs sur des connexions mobiles.

- Cache efficace: Des mécanismes de cache sont utilisés pour accélérer les réponses du serveur et réduire la charge du backend.

- Bonne configuration SSL/TLS: Le serveur utilise TLS 1.2 et TLS 1.3 avec des chiffrements sécurisés, et le certificat SSL est valide.

Points Faibles

- Mots de passe par défaut: L'interface d'administration est accessible avec un identifiant et un mot de passe par défaut admin/admin, ce qui constitue une vulnérabilité majeure.

- Accès public à l'interface d'administration: L'interface d'administration est accessible via le port 8443, exposant ainsi le serveur à des attaques potentielles.

- Absence d'authentification à double facteur (2FA): L'interface d'administration ne dispose pas de 2FA, ce qui rend l'accès plus vulnérable aux attaques par force brute.

- Version obsolète de LiteSpeed et WordPress: Des vulnérabilités peuvent exister dans la version de LiteSpeed utilisée et dans la version obsolète de WordPress (6.6.2).

- Présence de traces Drupal: Un en-tête Drupal a été trouvé dans la réponse HTTP, bien que le site soit sous WordPress. Cela pourrait exposer des informations sensibles.

- Fichiers de configuration mal sécurisés: Le fichier robots.txt pourrait exposer des répertoires inutiles aux moteurs de recherche, augmentant le risque de divulgation d'informations sensibles.

- Exposition de l'API REST de WordPress: L'API REST (wp-json) est exposée, ce qui peut constituer une porte d'entrée pour les attaquants si elle n'est pas correctement sécurisée.

4.3 Recommandations

Voici les recommandations pour améliorer la sécurité du système :

- Modifier les mots de passe par défaut: Il est crucial de remplacer les mots de passe par défaut dans l'interface d'administration par des mots de passe robustes.

- Restreindre l'accès à l'interface d'administration: Limiter l'accès à l'interface d'administration à des adresses IP spécifiques et configurer un pare-feu pour protéger le port 8443.

- Activer l'authentification à double facteur (2FA): Mettre en œuvre l'authentification à double facteur pour tous les utilisateurs ayant accès à l'interface d'administration.

- Mettre à jour LiteSpeed et WordPres: Mettre à jour la version de LiteSpeed et de WordPress pour corriger les vulnérabilités de sécurité.

**- Supprimer les traces de Drupa Vérifier et supprimer toutes les traces de Drupal du serveur afin d'éviter les fuites d'informations.

- Sécuriser le fichier robots.txt: S'assurer que le fichier robots.txt ne divulgue pas d'informations sensibles ou de répertoires inutiles.

- Sécuriser l'API REST de WordPress: Restreindre ou sécuriser l'accès à l'API REST (wp-json) pour éviter l'exploitation de cette interface.

Conclusion

L'audit de sécurité du système d'information révèle une architecture robuste et bien optimisée avec plusieurs bonnes pratiques en matière de performance et de sécurité. Cependant, plusieurs vulnérabilités ont été identifiées, notamment des mots de passe par défaut, l'accès public à l'interface d'administration et l'absence d'authentification à double facteur. En mettant en œuvre les recommandations proposées, le site pourra améliorer considérablement sa sécurité et réduire les risques potentiels.