

Rapport d'Audit de Sécurité – Site WordPress

1. Informations générales

Client : Exemple SARL

URL auditée : <https://www.exemple-site.fr>

Date de l'audit : 18 juillet 2025

Auditeur : Maelström Cybersecurity

2. Résumé exécutif

Cet audit a pour objectif d'évaluer la sécurité générale du site WordPress. Les tests ont mis en évidence plusieurs vulnérabilités critiques ainsi que des configurations à améliorer. Un ensemble de recommandations est fourni afin d'y remédier efficacement.

3. Vulnérabilités détectées

- Plugin vulnérable détecté

Le plugin 'XYZ Contact Form' utilise une version connue pour contenir une faille XSS.

- Mises à jour manquantes

Le noyau WordPress et 3 plugins ne sont pas à jour.

- Accès admin non protégé

L'URL /wp-admin est publique sans CAPTCHA ou limitation de tentative.

- Mot de passe faible

Un utilisateur admin utilise un mot de passe facilement devinable.

4. Recommandations

- Mettre à jour WordPress, les thèmes et plugins dès que possible.
- Remplacer le plugin 'XYZ Contact Form' par un plugin maintenu et sécurisé.
- Configurer une protection (reCAPTCHA, limitation d'accès) sur /wp-admin.
- Imposer des mots de passe forts pour tous les utilisateurs.

- Installer un pare-feu applicatif tel que Wordfence.
- Effectuer des scans réguliers avec WPScan ou un autre outil automatisé.

5. Conclusion

Le site présente des failles critiques qu'il convient de corriger rapidement. Une fois ces éléments sécurisés, un audit complémentaire peut être envisagé afin d'assurer une protection continue.