Audit de sécurité WordPress - Analyse pré-mise en production

Rapport technique et plan de remédiation validé par un expert sécurité

Par **Eddy AZEBAZE**

Ce rapport présente l'évaluation complète de la sécurité d'un site WordPress avant sa mise en production, identifiant les vulnérabilités potentielles et proposant un plan de remédiation détaillé pour garantir une protection optimale contre les cybermenaces.

Contexte stratégique

Objectif

Évaluer la sécurité d'un site WordPress public avant sa mise en production.

Contexte

Éviter les fuites de données, renforcer la posture cybersécurité et garantir la conformité réglementaire (RGPD, bonnes pratiques OWASP).

Méthode

Utilisation combinée d'outils d'analyse automatisée (OWASP ZAP, HTTP Observatory, SecurityHeaders) pour identifier et prioriser les risques.

Méthodologie d'audit en 4 étapes

Cadrage

Définition des objectifs et du périmètre.

Scans automatisés

OWASP ZAP, HTTP Observatory, SecurityHeaders.

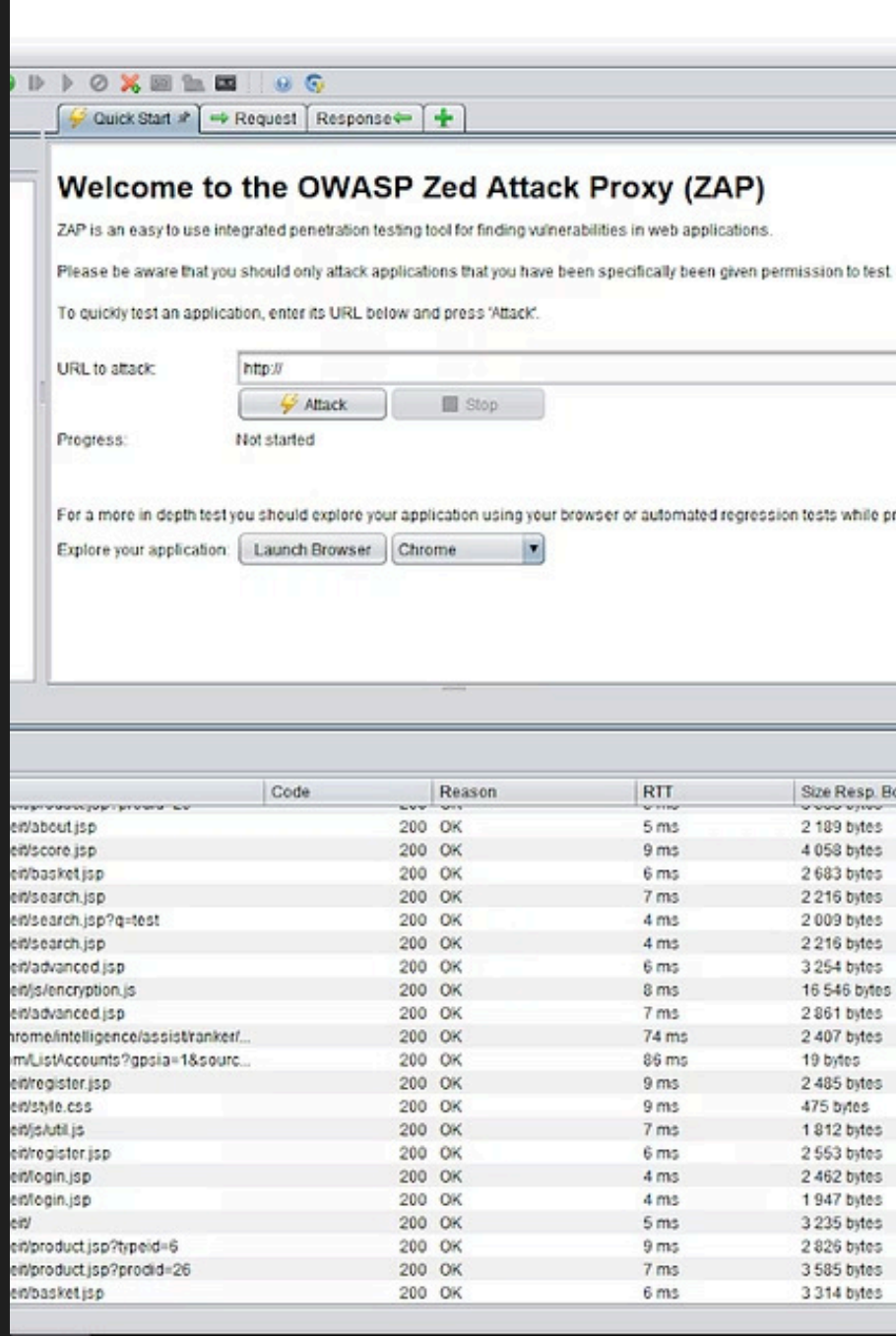
Analyse des résultats

Classification des vulnérabilités (critique, moyenne, faible).

Plan de remédiation

Recommandations concrètes validées par un expert sécurité.

Notre approche méthodique garantit une évaluation complète et structurée de la sécurité du site WordPress, permettant d'identifier efficacement les vulnérabilités et de proposer des solutions adaptées.



Résultats principaux de l'audit

OWASP ZAP

4 alertes (1 critique, 2 moyennes, 1 faible)

HTTP Observatory

Score F (0/100)

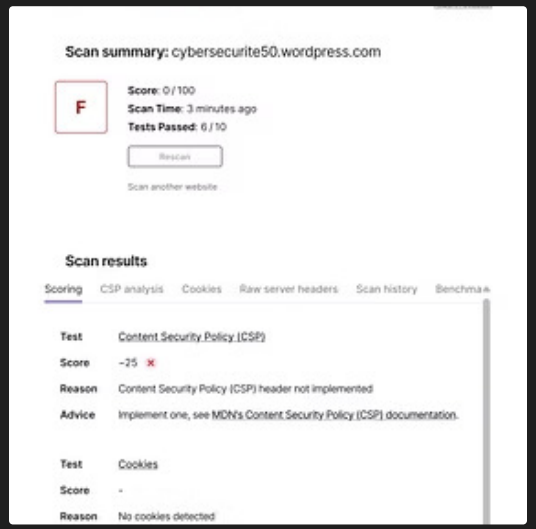
SecurityHeaders

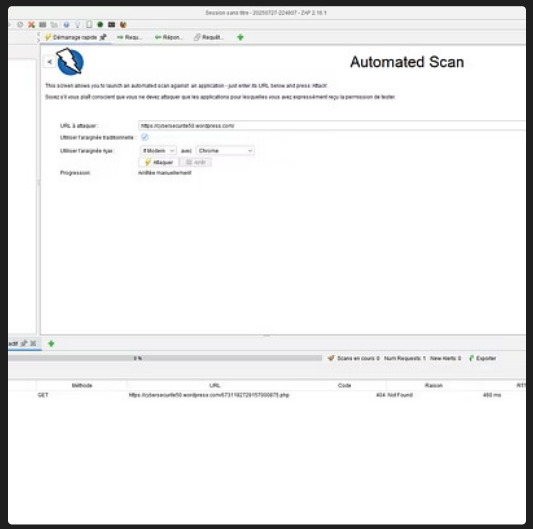
Score D

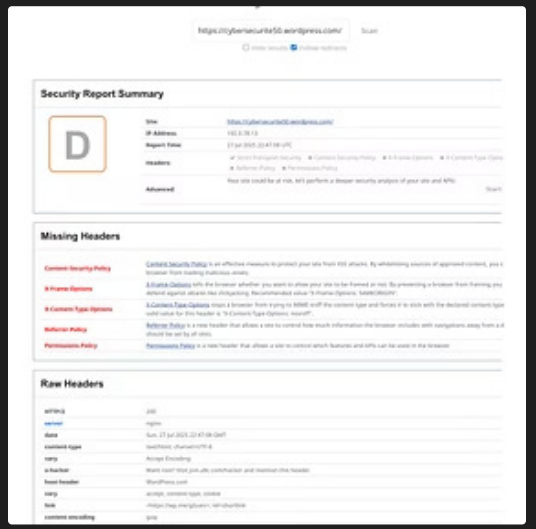
Vulnérabilités majeures identifiées : contenu mixte, absence de CSP, HSTS et Referrer-Policy.

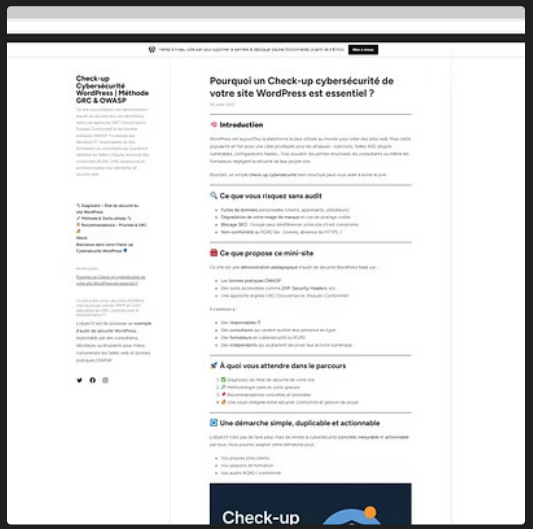
Outil	Score	Risques principaux
OWASP ZAP	4 alertes	Contenu mixte, headers manquants
HTTP Observatory	F (0/100)	Pas de CSP, HSTS manquant
SecurityHeaders	D	CSP, Referrer-Policy absents

Captures d'écran des résultats









Ces captures d'écran illustrent les différentes vulnérabilités identifiées lors de l'audit, notamment les scores insuffisants obtenus avec les outils d'analyse et les problèmes de sécurité détectés sur le site WordPress.

Plan de remédiation & Ressources

Forcer HTTPS et supprimer le contenu mixte.

Ajouter les en-têtes CSP, HSTS, X-Frame-Options.

Activer un plugin de sécurité (WP Cerber, HTTP Headers).

Mettre à jour le cœur WordPress et les extensions.

Activer un WAF (Cloudflare).

Rapport complet

Ce document est le rapport détaillé pour une analyse approfondie des résultats et des recommandations.

Projet GitHub

Consultez le projet sur GitHub Pages pour accéder à toutes les ressources et suivre les mises à jour.