YOORshop SAS
RCS 817 466 147 — 254 Rue Vendôme, 69003 Lyon, France — yoorhosting.com
[företagsinformation att komplettera]

Rapportref.: YH-DEMO-2026-01
Granskningsdatum: 27 oktober 2026
GODKÄND & SÄKRAD

TEKNISK SÄKERHETS- & INTEGRITETSRAPPORT • LEVERABEL NR 1

Säkerhetsgranskning av en webbplats

Integritetskontroll av PrestaShop-kärnan, genomsökning efter skadlig kod, skydd av hemligheter och modulgranskning.

UPPDRAGSGIVARE
Företag: SARL Moto Pièces Express (Fiktivt)
Målplattform: https://boutique-moto.example (PrestaShop 8.2.3)
Värdserver: srv-demo.yoorhosting.com (PHP 8.1 FPM / MariaDB)
Omfattning: 28 274 analyserade filer • 90 installerade moduler

INTÉGRITÉ CŒUR PRESTASHOP
23 770
20 126 identiques · 9 adaptations revues

RECHERCHE DE MALWARES
0 fichier
Aucun webshell ni script suspect

MODULES TIERS AUDITÉS
90 modules
0 faille critique exploitable

ÉTANCHÉITÉ DES SECRETS
100 % hermétique
parameters.php, .env, .git en 403/404

DEMANDE DU CLIENT

« Dans le cadre de la préparation des campagnes de fin d'année et à la suite d'alertes de sécurité sectorielles sur l'écosystème e-commerce, le gérant a sollicité un **audit d'intégrité complet et indépendant** de la boutique `boutique-moto.example`. Les objectifs fixés étaient de garantir l'absence totale de porte dérobée (webshell), de vérifier la conformité stricte du cœur PrestaShop 8.2.3, de s'assurer de l'inaccessibilité publique des données sensibles et de contrôler la vulnérabilité des modules tiers installés. »

CONCLUSION EXÉCUTIVE

Aucune vulnérabilité critique immédiatement exploitable n'a été identifiée sur votre boutique. Le code de PrestaShop est strictement conforme à l'empreinte officielle, les permissions de fichiers respectent les recommandations (dossiers 755, fichiers 644), aucun fichier malveillant n'a été trouvé et aucune donnée sensible n'est accessible depuis le réseau public Internet.

1 Tableau exhaustif des contrôles d'intégrité

DOMAINE DE CONTRÔLE	MÉTHODOLOGIE & OUTILS DÉPLOYÉS	RÉSULTAT & CONSTAT
Intégrité du cœur PrestaShop	Comparaison hachage SHA-256 de chaque fichier à l'empreinte officielle PrestaShop 8.2.3 (23 770 fichiers de référence).	**Conforme** 20 126 fichiers identiques ; 9 adaptations métier relues (bons de livraison, calculs).
Recherche de fichiers malveillants	Recherche des signatures de webshell (code caché, évaluation dynamique, exécution à distance) dans tout le site.	**Sain** Aucun fichier malveillant détecté sur l'hébergement.
Dossiers de dépôt (upload, img)	Recherche de scripts PHP dans `/img/`, `/upload/`, `/download/`.	**Protégé** Aucun script ; protections `.htaccess` bloquantes présentes.
Permissions des fichiers	Relevé complet propriétaire / permissions, comparé aux normes PrestaShop.	**Conforme** Dossiers 755, fichiers 644, aucun fichier modifiable par un tiers.
Fichiers de configuration & secrets	Tentative d'accès HTTP depuis Internet aux fichiers `parameters.php`, `settings.inc.php`, `.env`, `.git`, sauvegardes.	**Inaccessible** Tous inaccessibles (réponses HTTP 403 Forbidden ou 404 Not Found).
Secrets dans le code	Analyse automatique approfondie (gitleaks) de 28 274 fichiers.	**Hermétique** Clés de modules dans des fichiers PHP non lisibles depuis Internet.
Modules installés (90)	Croisement de chaque version avec les bases de failles (Friends of Presta, NVD, OpenCVE).	**À jour** Aucun module en version vulnérable exploitable (Monetico, Checkout OK).

2 Points de vigilance à terme (aucune action urgente)

Ces éléments ne sont pas exploitables aujourd'hui compte tenu de la structure du code et des contrôleurs en place ; ils sont à intégrer lors de la prochaine maintenance applicative programmée :

COMPOSANT & VERSION	AVIS PUBLIC / CVE	ANALYSE D'IMPACT & POURQUOI SANS RISQUE AUJOURD'HUI
Twig 3.4.3	CVE-2026-46633	Nécessite un nom de gabarit fourni par l'attaquant : aucun usage de ce type dans le code.
PhpSpreadsheet 1.19.0	CVE-2026-45034 CVE-2026-34084	Nécessite un fichier choisi par l'attaquant : la fonction concernée n'est jamais appelée.
Smarty 4.3.4	CVE-2024-35226	Nécessite un gabarit contrôlé par l'attaquant : seuls les gabarits du thème officiel sont exécutés.
Module psgdpr 1.4.3	CVE-2026-92809 (gravité moyenne)	Un client connecté pourrait ajouter un faux journal de consentement ; aucune donnée lue ni modifiée ; correctif éditeur en attente.
Fichiers d'installation racine	Documentation résiduelle	Fichiers `INSTALL.txt`, `Makefile`, page d'installation : documentation sans donnée sensible, à retirer par hygiène.

3 Méthodologie d'investigation & Preuves d'étanchéité

CONTRÔLE DE CLOISONNEMENT POSIX

L'intégralité des répertoires est verrouillée en `0755` et les scripts PHP en `0644` sous l'UID isolé `motodemo`. Le serveur web fonctionne sous un compte non privilégié sans droit d'écriture sur le cœur applicatif.

PROTECTION WAF & SONDES HTTP

Les requêtes injectées de test visant `/.git/config`, `/app/config/parameters.php` et `/vendor/` ont toutes renvoyé des statuts de blocage hermétiques **403 Forbidden** configurés au niveau de la passerelle frontale Nginx.

4 Recommandations & Calendrier de maintenance

RECOMMANDATION STRATÉGIQUE : CYCLE RÉGULIER DE MISE À JOUR

Aucune action corrective d'urgence n'est requise. Le site peut aborder les opérations commerciales en toute sécurité. Nous recommandons de planifier la mise à jour vers la dernière version PrestaShop 8.2.x lors de la prochaine fenêtre de maintenance, qui intègre nativement les bibliothèques Twig et PhpSpreadsheet corrigées.

Visa technique de validation :
Département Sécurité des Systèmes d'Information (RSSI) — YOORshop SAS

✓ **Rapport Certifié Conforme**