YOORshop SAS

RCS 817 466 147 — 254 Rue Vendôme, 69003 Lyon, France — yoorhosting.com

[Unternehmensangaben zu ergänzen]

Bericht-Nr.: YH-DEMO-2026-01
Auditdatum: 27. Oktober 2026

KONFORM & GESICHERT

SICHERHEITS- & INTEGRITÄTSBERICHT • ERGEBNIS NR. 1

Website-Sicherheitsaudit

Integritätsprüfung des PrestaShop-Kerns, Malware-Scan, Schutz vertraulicher Daten und Modul-Audit.

AUFTRAGGEBER

Unternehmen: SARL Moto Pièces Express (Fiktiv)
Zielplattform: https://boutique-moto.example (PrestaShop 8.2.3)
Host-Server: srv-demo.yoorhosting.com (PHP 8.1 FPM / MariaDB)
Umfang: 28 274 geprüfte Dateien • 90 installierte Module

PRESTASHOP-KERNINTEGRITÄT
23 770
20 126 identisch · 9 Anpassungen geprüft

MALWARE-SUCHE
0 Dateien
Keine Webshells oder Schadskripte

GEPRÜFTE DRITTMODULE
90 Module
0 ausnutzbare kritische Lücken

GEHEIMNISSCHUTZ
100 % dicht
parameters.php, .env, .git mit 403/404

KUNDENANFRAGE

„Zur Vorbereitung des Jahresendgeschäfts und nach branchenweiten Sicherheitswarnungen im E-Commerce beauftragte die Geschäftsführung ein **vollständiges, unabhängiges Integritätsaudit** des Shops `boutique-moto.example`. Ziel war es, Backdoors (Webshells) auszuschließen, die Konformität des PrestaShop-Kerns 8.2.3 zu bestätigen, den öffentlichen Zugriff auf sensible Daten zu unterbinden und alle Drittmodule auf Schwachstellen zu prüfen."

ZUSAMMENFASSUNG (EXECUTIVE SUMMARY)

Auf Ihrem Shop wurde keine unmittelbar ausnutzbare kritische Schwachstelle festgestellt. Der PrestaShop-Code entspricht exakt der offiziellen Referenz, die Dateirechte sind normgerecht (Ordner 755, Dateien 644), es wurde keine Schadsoftware gefunden und sensible Daten sind aus dem Internet unzugänglich.

1 Vollständige Übersicht der Integritätsprüfungen

PRÜFBEREICH	METHODIK & EINGESETZTE WERKZEUGE	ERGEBNIS & BEFUND
PrestaShop-Kernintegrität	SHA-256-Prüfsummenabgleich jeder Datei mit dem offiziellen PrestaShop 8.2.3 Release (23 770 Referenzdateien).	**Konform** 20 126 identische Dateien; 9 fachliche Anpassungen einzeln geprüft (Lieferscheine, Berechnungen).
Suche nach Schaddateien	Signaturscan nach Webshells (verschleierter Code, dynamische Auswertung, Remote-Ausführung) im gesamten Shop.	**Sauber** Keine schädliche Datei auf dem Hosting-Konto gefunden.
Upload-Ordner (upload, img)	Suche nach ausführbaren PHP-Skripten in `/img/`, `/upload/`, `/download/`.	**Geschützt** Keine Skripte; blockierende `.htaccess`-Regeln aktiv.
Dateiberechtigungen	Vollständige Erfassung von Eigentümer und POSIX-Rechten, abgeglichen mit PrestaShop-Vorgaben.	**Konform** Ordner 755, Dateien 644, keine Datei durch Dritte beschreibbar.
Konfigurationsdateien & Secrets	Externe HTTP-Zugriffstests auf `parameters.php`, `settings.inc.php`, `.env`, `.git`, Backups.	**Gesperrt** Alle unzugänglich (HTTP 403 Forbidden oder 404 Not Found).
Geheimnisse im Quellcode	Automatisierte Tiefenanalyse (gitleaks) über 28 274 Dateien.	**Abgeschirmt** Modulschlüssel liegen in öffentlich nicht lesbaren PHP-Dateien.
Installierte Module (90)	Versionsabgleich mit öffentlichen Schwachstellendatenbanken (Friends of Presta, NVD, OpenCVE).	**Aktuell** Kein Modul in ausnutzbar verwundbarer Version (Monetico, Checkout OK).

2 Mittelfristige Beobachtungspunkte (kein dringender Handlungsbedarf)

Diese gemeldeten Punkte sind aufgrund der Code-Architektur aktuell nicht ausnutzbar und sollten beim nächsten regulären Wartungsfenster eingeplant werden:

KOMPONENTE & VERSION	ÖFFENTLICHE MELDUNG / CVE	AUSWIRKUNGSANALYSE & WARUM HEUTE KEIN RISIKO BESTEHT
Twig 3.4.3	CVE-2026-46633	Setzt einen vom Angreifer übergebenen Template-Namen voraus: im Code nirgends verwendet.
PhpSpreadsheet 1.19.0	CVE-2026-45034 CVE-2026-34084	Erfordert eine vom Angreifer gewählte Datei: die betroffene Funktion wird im Shop nie aufgerufen.
Smarty 4.3.4	CVE-2024-35226	Erfordert ein vom Angreifer kontrolliertes Template: es werden nur offizielle Theme-Templates ausgeführt.
Modul psgdpr 1.4.3	CVE-2026-92809 (mittlerer Schweregrad)	Ein eingeloggter Kunde könnte einen falschen Einwilligungseintrag erzeugen; kein Lese-/Schreibzugriff auf Daten; Hersteller-Patch steht aus.
Installationsdateien im Root	Restdokumentation	Dateien `INSTALL.txt`, `Makefile`, Installationsseite: Dokumentation ohne sensible Daten, aus Hygienegründen zu entfernen.

3 Untersuchungsmethodik & Abschottungsnachweise

POSIX-ISOLATIONSPRÜFUNG

Sämtliche Verzeichnisse sind auf `0755` und PHP-Skripte auf `0644` unter der isolierten UID `motodemo` gesetzt. Der Webserver läuft unter einem unprivilegierten Konto ohne Schreibrechte auf den Anwendungskern.

WAF-SCHUTZ & HTTP-TESTSONDEN

Gezielte Testabfragen auf `/.git/config`, `/app/config/parameters.php` und `/vendor/` wurden vom vorgeschalteten Nginx-Gateway lückenlos mit **403 Forbidden** abgewiesen.

4 Empfehlungen & Wartungsfahrplan

STRATEGISCHE EMPFEHLUNG: REGULÄRER UPDATE-ZYKLUS

Es sind keine Notfallmaßnahmen erforderlich. Der Shop kann das Weihnachtsgeschäft sicher abwickeln. Wir empfehlen, im nächsten Wartungsfenster das Update auf die neueste PrestaShop-Version 8.2.x einzuplanen, welche die aktualisierten Bibliotheken Twig und PhpSpreadsheet direkt enthält.

Technische Prüfungsfreigabe:
Abteilung Informationssicherheit (CISO) — YOORshop SAS

✓ Zertifizierter Prüfbericht