YOORshop SAS

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

`[company details to be completed]`

Report Ref.: YH-DEMO-2026-01
Audit Date: October 27, 2026

COMPLIANT & SECURE

SECURITY & INTEGRITY ENGINEERING REPORT • DELIVERABLE #1

Website Security Audit

PrestaShop core integrity check, malware scan, secret exposure testing, and third-party module audit.

RECIPIENT CLIENT

Company: SARL Moto Pièces Express (Fictional)
Target Platform: https://boutique-moto.example (PrestaShop 8.2.3)
Host Server: srv-demo.yoorhosting.com (PHP 8.1 FPM / MariaDB)
Scope: 28,274 files analyzed • 90 installed modules

PRESTASHOP CORE INTEGRITY
23,770
20,126 identical · 9 custom edits reviewed

MALWARE SCAN
0 files
No webshells or suspicious scripts

AUDITED 3RD-PARTY MODULES
90 modules
0 exploitable critical vulnerabilities

SECRET CONTAINMENT
100% Sealed
parameters.php, .env, .git return 403/404

CLIENT REQUEST

"Ahead of peak year-end sales campaigns and following industry-wide e-commerce security alerts, management requested a **comprehensive, independent integrity audit** of the `boutique-moto.example` online store. The objectives were to guarantee the complete absence of backdoors (webshells), verify strict compliance of the PrestaShop 8.2.3 core, ensure sensitive configuration data cannot be accessed publicly, and check all installed third-party modules for known vulnerabilities."

EXECUTIVE SUMMARY

No immediately exploitable critical vulnerability was identified on your online store. The PrestaShop codebase strictly matches the official release fingerprint, file permissions follow best practices (directories 755, files 644), no malicious file was found, and no sensitive data is accessible from the public Internet.

1 Comprehensive Integrity & Security Check Matrix

CONTROL DOMAIN	METHODOLOGY & DEPLOYED TOOLS	RESULT & FINDING
PrestaShop Core Integrity	SHA-256 hash comparison of every file against the official PrestaShop 8.2.3 release (23,770 reference files).	**Compliant** 20,126 identical files; 9 business customizations reviewed line-by-line (delivery slips, calculations).
Malware & Webshell Scan	Signature scan for webshells (obfuscated code, dynamic evaluation, remote code execution) across the entire site.	**Clean** No malicious file detected anywhere on the hosting account.
Upload Directories (upload, img)	Scan for executable PHP scripts inside `/img/`, `/upload/`, `/download/`.	**Protected** No scripts found; blocking `.htaccess` rules active.
File Permissions	Full ownership and POSIX permission inventory compared against PrestaShop security standards.	**Compliant** Directories 755, files 644; no file writable by third parties.
Configuration Files & Secrets	External HTTP access attempts against `parameters.php`, `settings.inc.php`, `.env`, `.git`, and backups.	**Inaccessible** All blocked (HTTP 403 Forbidden or 404 Not Found responses).
Secrets in Source Code	Automated deep secret scan (gitleaks) across 28,274 files.	**Sealed** Module keys stored in PHP files unreadable from the Internet.
Installed Modules (90)	Cross-check of every module version against vulnerability databases (Friends of Presta, NVD, OpenCVE).	**Up to date** No module running an exploitable vulnerable version (Monetico, Checkout OK).

2 Medium-Term Watch Items (No Urgent Action Required)

Given the current codebase structure and active controllers, the following public advisories are not exploitable today; they should be addressed during the next scheduled maintenance window:

COMPONENT & VERSION	PUBLIC ADVISORY / CVE	IMPACT ANALYSIS & WHY THERE IS NO RISK TODAY
Twig 3.4.3	CVE-2026-46633	Requires an attacker-supplied template name: no such usage exists anywhere in the codebase.
PhpSpreadsheet 1.19.0	CVE-2026-45034 CVE-2026-34084	Requires an attacker-supplied file passed to a specific function that is never called on the store.
Smarty 4.3.4	CVE-2024-35226	Requires an attacker-controlled template: only official theme templates are executed.
Module psgdpr 1.4.3	CVE-2026-92809 (medium severity)	An authenticated customer could add a bogus consent log entry; no data can be read or altered; vendor patch pending.
Root Install Files	Residual documentation	`INSTALL.txt`, `Makefile`, install page: static documentation with no sensitive data, to be removed as good hygiene.

3 Investigation Methodology & Containment Proofs

POSIX ISOLATION CONTROL

All directories are locked to `0755` and PHP scripts to `0644` under the isolated UID `motodemo`. The web server runs under an unprivileged account without write permissions over the application core.

WAF PROTECTION & HTTP PROBES

Injected test requests targeting `/.git/config`, `/app/config/parameters.php`, and `/vendor/` all returned strict **403 Forbidden** blocking statuses enforced by the front-end Nginx gateway.

4 Recommendations & Maintenance Schedule

STRATEGIC RECOMMENDATION: REGULAR UPDATE CYCLE

No emergency corrective action is required. The store is ready for peak commercial operations. We recommend scheduling an update to the latest PrestaShop 8.2.x minor release during the next maintenance window, which natively bundles the patched Twig and PhpSpreadsheet libraries.

Technical Validation Sign-off:
Information Systems Security Department (CISO) — YOORshop SAS

✓ Certified Compliant Report