YOORshop SAS

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

`[dati aziendali da completare]`

Rif. rapporto: YH-DEMO-2026-01
Data di audit: 27 ottobre 2026

● **CONFORME E SICURO**

RAPPORTO DI INGEGNERIA DI SICUREZZA E INTEGRITÀ · LIVRABILE N. 1

Audit di sicurezza di un sito web

Controllo di integrità del core PrestaShop, ricerca di malware, protezione dei segreti e audit dei moduli.

CLIENTE DESTINATARIO

Società: SARL Moto Pièces Express (Fittizio)
Piattaforma target: https://boutique-moto.example (PrestaShop 8.2.3)
Server host: srv-demo.yoorhosting.com (PHP 8.1 FPM / MariaDB)
Perimetro: 28 274 file analizzati • 90 moduli installati

INTEGRITÀ CORE PRESTASHOP
23 770
20 126 identici · 9 adattamenti verificati

RICERCA MALWARE
0 file
Nessuna webshell né script sospetto

MODULI TERZI VERIFICATI
90 moduli
0 falle critiche sfruttabili

PROTEZIONE DEI SEGRETI
100 % ermetica
parameters.php, .env, .git in 403/404

RICHIESTA DEL CLIENTE

«In vista delle campagne commerciali di fine anno e a seguito di allerte di sicurezza nel settore e-commerce, la direzione ha richiesto un **audit di integrità completo e indipendente** dello store `boutique-moto.example`. Gli obiettivi prefissati erano garantire l'assenza totale di backdoor (webshell), verificare la rigorosa conformità del core PrestaShop 8.2.3, accertare l'inaccessibilità pubblica dei dati sensibili e controllare la vulnerabilità dei moduli di terze parti installati.»

SINTESI ESECUTIVA

Non è stata rilevata alcuna vulnerabilità critica immediatamente sfruttabile sul vostro negozio. Il codice di PrestaShop è pienamente conforme all'impronta ufficiale, i permessi dei file rispettano le raccomandazioni (cartelle 755, file 644), non è stato trovato alcun file malevolo e nessun dato sensibile è accessibile dalla rete Internet pubblica.

1 Tabella esaustiva dei controlli di integrità

AMBITO DI CONTROLLO	METODOLOGIA E STRUMENTI IMPIEGATI	RISULTATO E RISCONTRO
Integrità del core PrestaShop	Confronto hash SHA-256 di ogni file con l'impronta ufficiale PrestaShop 8.2.3 (23 770 file di riferimento).	**Conforme** 20 126 file identici; 9 adattamenti applicativi riletti (bolle di consegna, calcoli).
Ricerca di file malevoli	Scansione delle firme di webshell (codice offuscato, valutazione dinamica, esecuzione remota) su tutto il sito.	**Integro** Nessun file malevolo rilevato sull'account di hosting.
Cartelle di caricamento (upload, img)	Ricerca di script PHP eseguibili in `/img/`, `/upload/`, `/download/`.	**Protetto** Nessuno script; protezioni `.htaccess` bloccanti presenti.
Permessi dei file	Rilievo completo proprietario / permessi confrontato con gli standard PrestaShop.	**Conforme** Cartelle 755, file 644, nessun file modificabile da terzi.
File di configurazione e segreti	Tentativi di accesso HTTP da Internet a `parameters.php`, `settings.inc.php`, `.env`, `.git`, backup.	**Inaccessibile** Tutti inaccessibili (risposte HTTP 403 Forbidden o 404 Not Found).
Segreti nel codice sorgente	Analisi automatica approfondita (gitleaks) su 28 274 file.	**Ermetico** Chiavi dei moduli in file PHP non leggibili da Internet.
Moduli installati (90)	Incrocio di ogni versione con i database di vulnerabilità (Friends of Presta, NVD, OpenCVE).	**Aggiornato** Nessun modulo in versione vulnerabile sfruttabile (Monetico, Checkout OK).

2 Punti di attenzione a medio termine (nessuna azione urgente)

Questi elementi non sono sfruttabili oggi vista la struttura del codice e dei controller attivi; andranno integrati durante la prossima manutenzione applicativa programmata:

COMPONENTE E VERSIONE	AVVISO PUBBLICO / CVE	ANALISI D'IMPATTO E PERCHÉ OGGI NON PRESENTA RISCHI
Twig 3.4.3	CVE-2026-46633	Richiede un nome di template fornito dall'attaccante: nessun utilizzo di questo tipo nel codice.
PhpSpreadsheet 1.19.0	CVE-2026-45034 CVE-2026-34084	Richiede un file scelto dall'attaccante: la funzione interessata non viene mai richiamata.
Smarty 4.3.4	CVE-2024-35226	Richiede un template controllato dall'attaccante: vengono eseguiti solo i template del tema ufficiale.
Modulo psgdpr 1.4.3	CVE-2026-92809 (gravità media)	Un cliente autenticato potrebbe aggiungere un falso log di consenso; nessun dato letto né modificato; patch del fornitore in attesa.
File di installazione in root	Documentazione residua	File `INSTALL.txt`, `Makefile`, pagina d'installazione: documentazione priva di dati sensibili, da rimuovere per igiene.

3 Metodologia d'indagine e prove di isolamento

CONTROLLO DI ISOLAMENTO POSIX

Tutte le directory sono bloccate in `0755` e gli script PHP in `0644` sotto l'UID isolato `motodemo`. Il web server opera con un account non privilegiato senza diritti di scrittura sul core applicativo.

PROTEZIONE WAF E SONDE HTTP

Le richieste di test indirizzate a `/.git/config`, `/app/config/parameters.php` e `/vendor/` hanno restituito stati di blocco ermetici **403 Forbidden** configurati sul gateway frontale Nginx.

4 Raccomandazioni e calendario di manutenzione

RACCOMANDAZIONE STRATEGICA: CICLO REGOLARE DI AGGIORNAMENTO

Non è richiesto alcun intervento correttivo d'urgenza. Il sito può affrontare le operazioni commerciali in piena sicurezza. Raccomandiamo di pianificare l'aggiornamento all'ultima versione PrestaShop 8.2.x nella prossima finestra di manutenzione, che integra nativamente le librerie Twig e PhpSpreadsheet aggiornate.

Visto tecnico di validazione:
Dipartimento Sicurezza dei Sistemi Informativi (CISO) — YOORshop SAS

✓ **Rapporto Certificato Conforme**