YOORshop SAS

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

`[informații despre companie de completat]`

Ref. raport: YH-DEMO-2026-01
Data auditului: 27 octombrie 2026

● **CONFORM ȘI SECURIZAT**

RAPORT DE INGINERIE DE SECURITATE ȘI INTEGRITATE • LIVRABIL NR. 1

Audit de securitate al unui site web

Controlul integrității nucleului PrestaShop, scanare malware, etanșeitatea secretelor și auditul modulelor.

CLIENT DESTINATAR

Companie: SARL Moto Pièces Express (Fictiv)
Platformă țintă: https://boutique-moto.example (PrestaShop 8.2.3)
Server gazdă: srv-demo.yoorhosting.com (PHP 8.1 FPM / MariaDB)
Perimetru: 28 274 fișiere analizate • 90 module instalate

INTEGRITATE NUCLEU PRESTASHOP
23 770
20 126 identice · 9 adaptări verificate

CĂUTARE MALWARE
0 fișiere
Niciun webshell sau script suspect

MODULE TERȚE AUDITATE
90 module
0 vulnerabilități critice exploatabile

ETANȘEITATEA SECRETELOR
100 % etanș
parameters.php, .env, .git în 403/404

SOLICITAREA CLIENTULUI

„În cadrul pregătirii campaniilor comerciale de sfârșit de an și în urma alertelor de securitate din sectorul e-commerce, conducerea a solicitat un **audit de integritate complet și independent** al magazinului `boutique-moto.example`. Obiectivele stabilite au fost garantarea absenței totale a ușilor din spate (webshell), verificarea conformității stricte a nucleului PrestaShop 8.2.3, asigurarea inaccesibilității publice a datelor sensibile și controlul vulnerabilității modulelor terțe instalate.”

CONCLUZIE EXECUTIVĂ

Nu a fost identificată nicio vulnerabilitate critică imediat exploatabilă în magazinul dumneavoastră. Codul PrestaShop este strict conform cu amprenta oficială, permisiunile fișierelor respectă recomandările (directoare 755, fișiere 644), nu a fost găsit niciun fișier malițios și nicio dată sensibilă nu este accesibilă din rețeaua publică Internet.

1 Tabelul exhaustiv al controalelor de integritate

DOMENIU DE CONTROL	METODOLOGIE ȘI INSTRUMENTE UTILIZATE	REZULTAT ȘI CONSTATARE
Integritatea nucleului PrestaShop	Compararea hash-ului SHA-256 al fiecărui fișier cu amprenta oficială PrestaShop 8.2.3 (23 770 fișiere de referință).	**Conform** 20 126 fișiere identice; 9 adaptări de business revizuite individual (avize de livrare, calcule).
Căutarea fișierelor malițioase	Căutarea semnăturilor de webshell (cod ascuns, evaluare dinamică, execuție la distanță) în întregul site.	**Curat** Niciun fișier malițios detectat pe contul de găzduire.
Directoare de încărcare (upload, img)	Căutarea scripturilor PHP în `/img/`, `/upload/`, `/download/`.	**Protejat** Niciun script; protecții `.htaccess` blocante prezente.
Permisiunile fișierelor	Inventar complet proprietar / permisiuni, comparat cu normele PrestaShop.	**Conform** Directoare 755, fișiere 644, niciun fișier modificabil de către terți.
Fișiere de configurare și secrete	Tentative de acces HTTP din Internet la `parameters.php`, `settings.inc.php`, `.env`, `.git`, copii de siguranță.	**Inaccesibil** Toate inaccesibile (răspunsuri HTTP 403 Forbidden sau 404 Not Found).
Secrete în codul sursă	Analiză automată aprofundată (gitleaks) a 28 274 de fișiere.	**Etanș** Cheile modulelor sunt în fișiere PHP care nu pot fi citite din Internet.
Module instalate (90)	Corelarea fiecărei versiuni cu bazele de vulnerabilități (Friends of Presta, NVD, OpenCVE).	**Actualizat** Niciun modul în versiune vulnerabilă exploatabilă (Monetico, Checkout OK).

2 Puncte de vigilență pe termen mediu (nicio acțiune urgentă)

Aceste elemente nu sunt exploatabile astăzi datorită structurii codului și controlerelor active; ele urmează să fie tratate la următoarea mentenanță programată:

COMPONENTĂ ȘI VERSIUNE	AVIZ PUBLIC / CVE	ANALIZA IMPACTULUI ȘI DE CE NU EXISTĂ RISC ASTĂZI
Twig 3.4.3	CVE-2026-46633	Necesită un nume de șablon furnizat de atacator: nicio utilizare de acest tip în cod.
PhpSpreadsheet 1.19.0	CVE-2026-45034 CVE-2026-34084	Necesită un fișier ales de atacator: funcția vizată nu este apelată niciodată.
Smarty 4.3.4	CVE-2024-35226	Necesită un șablon controlat de atacator: sunt executate doar șabloanele temei oficiale.
Modul psgdpr 1.4.3	CVE-2026-92809 (gravitate medie)	Un client autentificat ar putea adăuga un jurnal fals de consimțământ; nicio dată citită sau modificată; patch-ul editorului în așteptare.
Fișiere de instalare în rădăcină	Documentație reziduală	Fișierele `INSTALL.txt`, `Makefile`, pagina de instalare: documentație fără date sensibile, de eliminat pentru igienă.

3 Metodologia de investigație și dovezile de izolare

CONTROLUL IZOLĂRII POSIX

Toate directoarele sunt blocate la `0755` și scripturile PHP la `0644` sub UID-ul izolat `motodemo`. Serverul web rulează sub un cont neprivilegiat, fără drept de scriere asupra nucleului aplicației.

PROTECȚIE WAF ȘI SONDE HTTP

Cererile de test care au vizat `/.git/config`, `/app/config/parameters.php` și `/vendor/` au returnat blocări etanșe **403 Forbidden** configurate la nivelul gateway-ului frontal Nginx.

4 Recomandări și calendarul de mentenanță

RECOMANDARE STRATEGICĂ: CICLU REGULAT DE ACTUALIZARE

Nu este necesară nicio acțiune corectivă de urgență. Site-ul poate aborda operațiunile comerciale în deplină siguranță. Recomandăm planificarea actualizării la ultima versiune PrestaShop 8.2.x în următoarea fereastră de mentenanță, care integrează nativ bibliotecile Twig și PhpSpreadsheet corectate.

Aviz tehnic de validare:
Departamentul Securitatea Sistemelor Informatice (CISO) — YOORshop SAS

✓ **Raport Certificat Conform**