YOORshop SAS

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

`[dane firmy do uzupełnienia]`

Ref. raportu: YH-DEMO-2026-01
Data audytu: 27 października 2026

● ZGODNY I BEZPIECZNY

RAPORT INŻYNIERII BEZPIECZEŃSTWA I INTEGRALNOŚCI · REZULTAT NR 1

Audyt bezpieczeństwa strony internetowej

Kontrola integralności rdzenia PrestaShop, skanowanie malware, szczelność sekretów i audyt modułów.

KLIENT DOCELOWY

Firma: SARL Moto Pièces Express (Fikcyjna)
Platforma: https://boutique-moto.example (PrestaShop 8.2.3)
Serwer hosta: srv-demo.yoorhosting.com (PHP 8.1 FPM / MariaDB)
Zakres: 28 274 sprawdzonych plików • 90 modułów

INTEGRALNOŚĆ PRESTASHOP
23 770
20 126 identycznych · 9 zmian sprawdzonych

SKANOWANIE MALWARE
0 plików
Brak webshelli i podejrzanych skryptów

ZBADANE MODUŁY ZEWN.
90 modułów
0 krytycznych luk do wykorzystania

SZCZELNOŚĆ SEKRETÓW
100 % szczelne
parameters.php, .env, .git zwracają 403/404

ZGŁOSZENIE KLIENTA

„W ramach przygotowań do kampanii sprzedażowych końca roku oraz po branżowych alertach bezpieczeństwa e-commerce, zarząd zlecił **pełny, niezależny audyt integralności** sklepu `boutique-moto.example`. Celem było potwierdzenie braku tylnych furtek (webshell), weryfikacja zgodności rdzenia PrestaShop 8.2.3, blokada publicznego dostępu do danych wrażliwych oraz kontrola podatności zainstalowanych modułów zewnętrznych."

PODSUMOWANIE WYKONAWCZE

W sklepie nie wykryto żadnej krytycznej podatności możliwej do bezpośredniego wykorzystania. Kod PrestaShop jest w pełni zgodny z oficjalnym wzorcem, uprawnienia plików spełniają normy (katalogi 755, pliki 644), nie znaleziono złośliwego oprogramowania, a dane wrażliwe są niedostępne z sieci publicznej.

1 Szczegółowe zestawienie kontroli integralności

OBSZAR KONTROLI	METODOLOGIA I UŻYTE NARZĘDZIA	WYNIK I USTALENIA
Integralność rdzenia PrestaShop	Porównanie skrótów SHA-256 każdego pliku z oficjalnym wydaniem PrestaShop 8.2.3 (23 770 plików wzorcowych).	**Zgodny** 20 126 plików identycznych; 9 adaptacji biznesowych sprawdzonych ręcznie (listy przewozowe, wyliczenia).
Wykrywanie złośliwych plików	Skanowanie sygnatur webshelli (ukryty kod, dynamiczna ewaluacja, zdalne wykonanie) w całym serwisie.	**Czysty** Brak złośliwych plików na koncie hostingowym.
Katalogi wgrywania (upload, img)	Poszukiwanie skryptów wykonywalnych PHP w `/img/`, `/upload/`, `/download/`.	**Chroniony** Brak skryptów; aktywne reguły blokujące `.htaccess`.
Uprawnienia plików	Pełny odczyt właścicieli i praw dostępu porównany z wytycznymi PrestaShop.	**Zgodny** Katalogi 755, pliki 644, brak plików z prawem zapisu dla osób trzecich.
Pliki konfiguracyjne i sekrety	Próby dostępu HTTP z Internetu do `parameters.php`, `settings.inc.php`, `.env`, `.git` i kopii.	**Niedostępny** Wszystkie zablokowane (odpowiedzi HTTP 403 Forbidden lub 404 Not Found).
Sekrety w kodzie źródłowym	Automatyczna głęboka analiza (gitleaks) 28 274 plików.	**Szczelny** Klucze modułów w plikach PHP nieczytelnych z Internetu.
Zainstalowane moduły (90)	Weryfikacja każdej wersji w bazach podatności (Friends of Presta, NVD, OpenCVE).	**Aktualny** Brak modułów w podatnej wersji możliwej do wykorzystania (Monetico, Checkout OK).

2 Punkty obserwacji średnioterminowej (brak pilnych działań)

Poniższe zgłoszenia nie są dziś możliwe do wykorzystania ze względu na strukturę kodu i aktywne kontrolery; należy je uwzględnić przy najbliższej planowej aktualizacji:

KOMPONENT I WERSJA	BIULETYN PUBLICZNY / CVE	ANALIZA WPŁYWU I DLACZEGO DZIŚ NIE STANOWI ZAGROŻENIA
Twig 3.4.3	CVE-2026-46633	Wymaga nazwy szablonu podanej przez atakującego: brak takiego użycia w kodzie sklepu.
PhpSpreadsheet 1.19.0	CVE-2026-45034 CVE-2026-34084	Wymaga pliku przekazanego przez atakującego: podatna funkcja nigdy nie jest wywoływana.
Smarty 4.3.4	CVE-2024-35226	Wymaga szablonu kontrolowanego przez atakującego: wykonywane są wyłącznie szablony oficjalnego motywu.
Moduł psgdpr 1.4.3	CVE-2026-92809 (średnia waga)	Zalogowany klient mógłby dodać fałszywy wpis zgody; brak odczytu i modyfikacji danych; oczekiwanie na łatkę wydawcy.
Pliki instalacyjne w katalogu głównym	Pozostała dokumentacja	Pliki `INSTALL.txt`, `Makefile`, strona instalacji: dokumentacja bez danych wrażliwych, do usunięcia dla higieny.

3 Metodologia dochodzeniowa i dowody izolacji

KONTROLA IZOLACJI POSIX

Wszystkie katalogi są zablokowane na `0755`, a skrypty PHP na `0644` pod izolowanym UID `motodemo`. Serwer WWW działa na koncie nieuprzywilejowanym bez praw zapisu w rdzeniu aplikacji.

OCHRONA WAF I SONDY HTTP

Testowe żądania wymierzone w `/.git/config`, `/app/config/parameters.php` oraz `/vendor/` zwróciły szczelne blokady **403 Forbidden** na bramie frontowej Nginx.

4 Zalecenia i harmonogram konserwacji

ZALECENIE STRATEGICZNE: REGULARNY CYKL AKTUALIZACJI

Nie są wymagane żadne pilne działania naprawcze. Sklep może bezpiecznie realizować kampanie sprzedażowe. Zalecamy zaplanowanie aktualizacji do najnowszej wersji PrestaShop 8.2.x w kolejnym oknie serwisowym, co automatycznie zaktualizuje biblioteki Twig i PhpSpreadsheet.

Zatwierdzenie techniczne audytu:
Dział Bezpieczeństwa Systemów Informacyjnych (CISO) — YOORshop SAS

✓ **Raport Certyfikowany**