YOORshop SAS

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

［会社情報追記欄］

レポート番号： YH-DEMO-2026-01
監査実施日： 2026年10月27日

● 適合・安全性確認済

セキュリティ＆完全性エンジニアリング報告書 • 成果物 #1

Webサイトセキュリティ監査

PrestaShopコアの完全性検証、マルウェア検査、機密情報の外部遮断テストおよびモジュール監査。

対象クライアント

企業名： SARL Moto Pièces Express（架空）
対象サイト： https://boutique-moto.example (PrestaShop 8.2.3)
ホストサーバー： srv-demo.yoorhosting.com (PHP 8.1 FPM / MariaDB)
監査範囲： 解析ファイル数 28,274件 • 導入モジュール 90個

PRESTASHOPコア完全性
23,770
20,126件一致 · 9件の独自改修を確認

マルウェア検査
0 件
Webシェル・不審スクリプトなし

外部モジュール監査
90 モジュール
悪用可能な重大脆弱性 0件

機密情報の遮断性
100 % 遮断
parameters.php, .env, .git は403/404

クライアントのご要望

「年末商戦キャンペーンの準備およびEC業界全体でのセキュリティ警告を受け、経営陣よりオンラインストア `boutique-moto.example` の**包括的かつ独立した完全性監査**をご依頼いただきました。目的は、バックドア（Webシェル）の完全な不在証明、PrestaShop 8.2.3コアの厳密な適合確認、機密データの外部アクセス遮断、および導入済みサードパーティ製モジュールの脆弱性点検です。」

エグゼクティブサマリー（結論）

貴社ストアにおいて、直ちに悪用可能な重大脆弱性は一切確認されませんでした。 PrestaShopのコードは公式ハッシュ値と厳密に一致し、ファイル権限も推奨基準（ディレクトリ755、ファイル644）に準拠しています。不正ファイルは検出されず、インターネットから機密データへのアクセスも完全に遮断されています。

1 完全性・セキュリティ監査結果一覧

監査項目	検証手法および使用ツール	結果および所見
PrestaShopコアの完全性	全ファイルのSHA-256ハッシュをPrestaShop 8.2.3公式リリース（基準23,770ファイル）と照合。	適合 20,126ファイルが完全一致。業務改修9件（納品書・計算処理）を個別精査し異常なし。
不正ファイルの探査	サイト全体でWebシェル署名（難読化コード、動的評価、遠隔コード実行）をスキャン。	健全 ホスティング領域内に不正ファイルは一切検出されず。
アップロード領域 (upload, img)	`/img/`、`/upload/`、`/download/` 内のPHPスクリプト有無を検査。	保護済 スクリプトなし。実行を阻止する `.htaccess` 保護が有効。
ファイル権限（パーミッション）	所有者および権限を網羅的に取得し、PrestaShop推奨基準と比較。	適合 ディレクトリ755、ファイル644。第三者が書き換え可能なファイルなし。
設定ファイル・機密情報	外部から `parameters.php`、`settings.inc.php`、`.env`、`.git` 等へのHTTPアクセスを試行。	アクセス不可 すべて遮断を確認（HTTP 403 Forbidden または 404 Not Found）。
コード内の機密キー検査	全28,274ファイルに対する自動シークレット検査（gitleaks）。	秘匿済 モジュールキーは外部から読み取り不能なPHPファイル内に格納。
導入済みモジュール (90個)	各バージョンを脆弱性DB（Friends of Presta、NVD、OpenCVE）と照合。	最新 悪用可能な脆弱バージョンなし（Monetico、Checkout等すべて正常）。

2 中期的な留意事項（緊急の対応は不要）

以下の公開情報は現在のコード構造および稼働コントローラー上、悪用不可能ですが、次回の定期メンテナンス時の更新を推奨します。

コンポーネント・版数	公開情報 / CVE	影響分析および現時点でリスクがない理由
Twig 3.4.3	CVE-2026-46633	攻撃者が指定したテンプレート名を処理する場合のみ該当。コード内に該当箇所なし。
PhpSpreadsheet 1.19.0	CVE-2026-45034 CVE-2026-34084	攻撃者が選択したファイルを特定関数で読み込む場合のみ該当。対象関数は未使用。
Smarty 4.3.4	CVE-2024-35226	攻撃者が制御するテンプレートの実行が条件。公式テーマのテンプレートのみ実行。
Module psgdpr 1.4.3	CVE-2026-92809（中程度）	ログイン顧客が同意ログを偽装追加できる可能性のみ。データの閲覧・改ざん不可。修正待ち。
ルートの初期導入ファイル	残存ドキュメント	`INSTALL.txt`、`Makefile` 等：機密情報を含まない文書ですが衛生上削除を推奨。

3 調査手法および隔離・遮断の証跡

POSIX権限による分離制御

全ディレクトリは `0755`、PHPスクリプトは `0644` に固定され、独立UID `motodemo` 下で管理されています。Webサーバーは非特権アカウントで動作し、コアへの書き込み権限を持ちません。

WAF保護およびHTTPプローブ検証

`/.git/config`、`/app/config/parameters.php`、`/vendor/` への疑似攻撃リクエストはすべてフロントエンドNginxゲートウェイにより **403 Forbidden** で完全に遮断されました。

4 推奨事項およびメンテナンス計画

戦略的推奨事項：定期アップデートサイクルの実施

緊急の是正措置は必要ありません。現在の状態で繁忙期の商用稼働を安全に継続いただけます。次回の計画メンテナンス枠にて、修正済みのTwigおよびPhpSpreadsheetライブラリを標準搭載した最新のPrestaShop 8.2.xマイナーバージョンへの更新を推奨いたします。

技術承認・検証サイン：
情報システムセキュリティ部門 (CISO) — YOORshop SAS

✓ 適合認定済レポート