RiskSignal powered by Ægis

Website Risk Exposure Audit

Demonstration Copy - Redacted

Client: [Redacted Shopify Brand]
URL Reviewed: [Redacted]
Date: February 17, 2026
Scope: Single-page (URL) snapshot
External Observable Review

Executive Summary

1. Overview

This assessment evaluates publicly observable signals related to accessibility and surface-level security configuration for the reviewed homepage.

The objective is to identify visible exposure patterns and provide a prioritized remediation path for internal decision-making.

2. Overall Risk Posture - Moderate

The site demonstrates baseline HTTPS enforcement and active Content Security Policy configuration. Several configuration gaps remain that exceed baseline browser hardening expectations.

This classification reflects current exposure across:

- Accessibility indicators
- Security header configuration
- TLS hygiene
- Cookie security flag behavior
- Public exposure patterns

This risk classification is based on the **RiskSignal Severity Framework**. (p.3)

3. Primary Exposure Areas

- Cookie security flag hardening inconsistencies
- Missing Referrer-Policy header
- Accessibility violations (3 detected)

Executive Summary

4. Recommended Remediation Order

Fix Now

- Harden cookie security flags
- Implement Referrer-Policy header

Fix Next

- Accessibility remediation
- Define Cache-Control policy

Monitor

- TLS certificate lifecycle management

5. Recommended Next Step

Address “Fix Now” items first. These provide the greatest reduction in exposure with minimal implementation effort.

Your development team can reference the Developer Appendix for technical guidance.

Scope Reminder:

This assessment reflects publicly observable signals only.
It does not include backend access, penetration testing, or legal certification.

Executive Summary

RiskSignal Severity Framework (Finding-Level)

Severity reflects exposure priority based on technical impact and likelihood under typical operating conditions.

- **High** - Credible observable exposure pattern with material downside; prioritize remediation.
- **Medium** - Meaningful weakness with plausible operational, security, or compliance impact.
- **Moderate** - Valid observable exposure signal with limited immediate impact; address in structured update cycle.
- **Minor** - Best-practice or hygiene improvement with low direct operational impact.

Key Findings

1. Cookie Security Flag Gaps

Observed

Cookies detected: 12
Secure flag missing: 8
HttpOnly flag missing: 8
SameSite attribute missing: 4

Business Impact

Incomplete cookie hardening increases potential session exposure risk in browser-based attack scenarios.

Recommended Action:

- Enforce Secure flag for HTTPS-only transmission
- Apply HttpOnly for session-related cookies
- Configure SameSite=Lax or Strict unless stricter behavior is validated

2. Missing Referrer-Policy Header

Observed

Referrer-Policy header not present.

Business Impact

Full URL paths may be exposed with external domains during cross-site navigation, exceeding baseline privacy hygiene standards.

Key Findings

Recommended Action:

- Implement `strict-origin-when-cross-origin` at CDN or server layer
- Verify header presence after deployment

3. Accessibility Violations (3)

Observed

- 3 automated accessibility violations detected
- No H1 element identified
- One color contrast issue present

Business Impact

Accessibility indicators may increase compliance exposure and reduce procurement confidence in regulated markets.

Recommended Action:

- Establish a proper H1 hierarchy
- Resolve contrast failures
- Validate semantic landmark structure

Developer Appendix

Technical Findings & Implementation Guidance

Client: [Redacted Shopify Brand]
URL: [Domain]
Date: February 17, 2026

Finding #1 - Cookie Security Flags

Category: Cookie / Exposure
Severity: Moderate

Observed Evidence:

- Secure flag missing on 8 cookies
- HttpOnly missing on 8 cookies
- SameSite missing on 4 cookies

Risk Context:
Improper cookie flags may allow session identifiers to be exposed through browser behavior or third-party contexts.

Recommended Action:

- Enforce Secure on HTTPS cookies
- Apply HttpOnly to session tokens
- Set SameSite=Lax or Strict where compatible

Implementation Notes:

- Shopify: configure via theme settings or edge/CDN rules
- Cloudflare/Nginx: apply header adjustments at edge
- Re-scan after deployment

Developer Appendix

Finding #2 - Referrer-Policy Header

Category: Security Header
Severity: Moderate

Observed Evidence:

- Header not detected

Risk Context:
Referrer data may expose full URL paths during cross-site navigation.

Recommended Action:

- Add `strict-origin-when-cross-origin`

Implementation Notes:

- Add header at CDN/server layer
- Validate via re-scan

Finding #3 - Accessibility Indicators

Category: Accessibility
Severity: Low-Moderate

Observed Evidence:

- Missing H1 structure
- Color contrast issue
- Automated rule flags

Risk Context:
May affect usability and contribute to compliance exposure.

Developer Appendix

Recommended Action:

- Implement proper heading hierarchy
- Resolve contrast failures

Implementation Notes:

- Adjust theme markup
- Validate using automated accessibility tools

Verification

After remediation, a **Verification Assessment** can be requested to confirm the following implementation changes based on the issues identified in this report:

- Cookie attributes (HttpOnly, Secure, SameSite) persist after deployment
- Referrer-Policy is implemented consistently across responses
- Previously flagged accessibility indicators show measurable reduction

If ongoing storefront updates are expected, **Monthly Operator Review Cycles** help maintain observable continuity without requiring repeated one-off verifications.

Scope & Limitations

This assessment reviews publicly observable accessibility indicators and surface-level security configuration signals.

Included:

- Accessibility rule indicators (automated)
- TLS certificate status
- Security header presence
- Cookie security flags
- Public exposure checks
- Configuration hygiene indicators

Excluded:

- Penetration testing or exploit attempts
- Backend or infrastructure access
- Code review or implementation work
- Legal advisory or compliance certification
- Guarantee of protection from regulatory action
- Continuous monitoring

RiskSignal reduces uncertainty by identifying visible exposure patterns.
It does not eliminate risk.

RiskSignal
Website Risk Exposure Audit
delivery@risksignal.io
https://risksignal.io

Prepared by
Jarvis Price
Founder, RiskSignal