BreachVector

Website Security Review

72

Target: velocity-commerce.demo
Normalized URL: https://velocity-commerce.demo
Completed: Mar 27, 2026, 6:52 AM
Origin: Seeded showcase

Executive summary

Velocity Commerce has the essentials of a modern HTTPS setup, but the security story is uneven. The biggest opportunity is to add a stronger browser policy layer and close smaller hygiene gaps before scaling traffic and integrations further.

Top findings

MEDIUM - HSTS header is missing

The application redirects to HTTPS but does not instruct browsers to keep using it automatically in future visits.
Remediation: Add Strict-Transport-Security with a staged rollout and includeSubDomains where appropriate.

LOW - Frame embedding protection is absent

No X-Frame-Options header was visible, which makes clickjacking protections less explicit for older browsers and simpler deployments.
Remediation: Add X-Frame-Options: DENY or SAMEORIGIN unless framing is required.

Technical narrative

The site already demonstrates good transport basics and a starter CSP, which makes it a strong foundation. Remaining work is mostly about consistency: HSTS, frame protections, and cookie flag standardization would tighten the public-facing posture without changing application behavior dramatically.

Remediation plan

Immediate - Enable HSTS

Pair the existing redirect with an HSTS header so browsers automatically keep subsequent sessions on HTTPS.

Next sprint - Add explicit anti-framing rules

Use X-Frame-Options or a CSP frame-ancestors directive, depending on whether legitimate framing is required.

Signal breakdown

HTTPS reachable: Yes
HTTP redirects to HTTPS: Yes
HTTPS status: 200
HTTP status: 308
TLS expiration: Aug 2, 2026, 12:00 PM
SPF: Not checked
DMARC: Not checked
MTA-STS: Not checked

Plain-English notes

X-Frame-Options

This header tells browsers whether another site is allowed to load your pages inside an iframe.