BreachVector

Website Security Review

54

Target: civic-portal.demo

Normalized URL: https://civic-portal.demo

Completed: Mar 27, 2026, 11:22 AM

Origin: Seeded showcase

Executive summary

Civic Portal is publicly reachable over HTTPS, but several foundational controls are absent or inconsistent. The site would benefit from transport hardening, stronger browser headers, and clearer cookie protections before it would present as security-mature to a stakeholder or procurement team.

Top findings

HIGH - HTTP does not force users onto HTTPS

The HTTP endpoint answered directly instead of redirecting to HTTPS, leaving room for users and old links to hit a weaker channel first.

Remediation: Configure a site-wide 301 or 308 redirect from HTTP to HTTPS.

MEDIUM - HSTS is not enabled

Strict-Transport-Security was not visible, so browsers are not instructed to keep using HTTPS after the first secure visit.

Remediation: Add a Strict-Transport-Security header with a meaningful max-age once HTTPS redirection is stable.

MEDIUM - Visible cookies are missing security flags

Two visible cookies did not include the full set of expected Secure, HttpOnly, or SameSite protections.

Remediation: Mark session-related cookies Secure, HttpOnly, and SameSite=Lax or Strict where possible.

Technical narrative

This surface is good enough for a live demo but not for a confident security posture story. HTTPS exists, yet transport controls are incomplete because HTTP remains open, HSTS is absent, and certificate renewal should be monitored closely due to the short remaining lifetime.

Remediation plan

Immediate - Force HTTPS everywhere

Add a permanent redirect from every HTTP request to the equivalent HTTPS URL and verify legacy paths behave consistently.

Immediate - Enable HSTS after redirect validation

Once HTTP redirect behavior is stable, instruct browsers to prefer HTTPS automatically.

Next sprint - Harden visible cookies

Review application and marketing cookies, then standardize Secure, HttpOnly, and SameSite flags.

Signal breakdown

HTTPS reachable: Yes
HTTP redirects to HTTPS: No
HTTPS status: 200
HTTP status: 200
TLS expiration: Apr 10, 2026, 12:00 PM
SPF: Present
DMARC: Missing
MTA-STS: Not checked
CAA: Not checked
robots.txt: Not detected
security.txt: Not detected

Plain-English notes

HSTS

HSTS tells the browser to keep using HTTPS so a visitor is less likely to land on an insecure version of the site later.

SameSite cookie

SameSite limits when browsers send cookies with cross-site requests, which helps reduce some account abuse and request forgery scenarios.