Web Security Configuration Audit - https://bryanrafaelbueno.github.io/audit-br-store/

- **Target:** `https://bryanrafaelbueno.github.io/audit-br-store/` `[200]` - **final:** `https://bryanrafaelbueno.github.io/audit-br-store/`

- **Host/port:** bryanrafaelbueno.github.io:443

- **Date (UTC):** 2026-09-05T06:06:49.834326+00:00

- **Tool:** reconpp 0.1.0 - passive checks only

Summary

{'PASS': 7, 'INFO': 4, 'WARN': 6, 'FAIL': 0}

WARN (6)

- **HSTS includeSubDomains** - HSTS present but includeSubDomains missing.

- Fix: For full coverage append '; includeSubDomains' (and preload when ready).

- **Content-Security-Policy** - No CSP set. XSS impact is amplified.

- Fix: Start with: default-src 'self'; script-src 'self'; object-src 'none'; frame-ancestors 'none'

- **X-Content-Type-Options** - Missing/incorrect. MIME sniffing can turn uploads into XSS.

- Fix: Add: X-Content-Type-Options: nosniff

- **Clickjacking (X-Frame-Options / frame-ancestors)** - No frame protection header and no CSP frame-ancestors.

- Fix: Add: Strict-Transport-Security-like header 'X-Frame-Options: DENY' or CSP 'frame-ancestors 'none''.

- **CORS response to Origin https://evil.example.org** - Wildcard ACAO allowed - sensitive data readable by any site.

- **CORS response to Origin null** - Wildcard ACAO allowed - sensitive data readable by any site.

INFO (4)

- **Referrer-Policy** - Not set. Referrer leakage into third-party links possible.

- Fix: Recommended: strict-origin-when-cross-origin

- **Permissions-Policy** - Not set (browser features like geolocation remain available).

- Fix: Consider: camera=(), microphone=(), geolocation=()

- **Server header / fingerprinting** - Server: GitHub.com. Fingerprintable technology stack.

- Fix: Consider generic values or removing the header to harden enumeration.

- **Set-Cookie** - No cookies observed in the base request. Session cookies may still exist per endpoint.

PASS (7)

- **HTTPS - no downgrade** - No downgrade in redirect chain.

- Fix: Final target: https://bryanrafaelbueno.github.io/audit-br-store/

- **TLSv1.2 negotiated** - ECDHE-RSA-AES128-GCM-SHA256 (TLSv1.2)

- **well-known: /robots.txt** - Search crawler rules: present (found).

- **well-known: /security.txt** - Vulnerability disclosure contact: not present (HTTP 404).

- **well-known: /.well-known/security.txt** - RFC 9116 disclosure contact: not present (HTTP 404).

- **well-known: /humans.txt** - Human-metadata file: not present (HTTP 404).

- **well-known: /sitemap.xml** - Site index: present (found).

Methodology

Checks are passive (non-intrusive) and cover: HTTP security headers, redirect chain, cookie flags, CORS exposure, TLS posture/certificate, exposed sensitive files and well-known resources (RFC 9116 security.txt). No fuzzing, brute force or exploit attempts were performed.