Web Security Baseline Assessment (WSBA) — example.com

Date (UTC): 2026-02-01
Assessment Type: Non-intrusive baseline (DNS, TLS, HTTP response headers)
Scope: https://example.com/
Authorization: Demonstration / training target used for methodology validation. No intrusive testing perfo
rmed.
Analyst: Archil Veltauri

Executive Summary

A baseline review identified multiple missing HTTP security headers that provide defense-in-depth protections in modern browsers. No exploitation was attempted. Recommendations focus on low-risk configuration improvemen s (response header hardening) and operational certificate monitoring.

Methodology (Non-Intrusive)

• DNS record snapshot (A/AAAA/MX/TXT)
• HTTPS response header capture
• TLS certificate subject/issuer/validity dates review
• No authentication testing, exploitation, or aggressive scanning performed

Key Findings (Prioritized)

ID	Finding	Severity	Recommendation
1	Missing HSTS (Strict-Transport-Security)	Medium	Enable HSTS after confirming HTTPS everywhere
2	Missing CSP (Content-Security-Policy)	Medium	Implement CSP (consider Report-Only first), then tighte n
3	Missing anti-clickjacking protection	Low–Medium	Add `frame-ancestors` via CSP or set `X-Frame-Option s`
4	Missing X-Content-Type-Options	Low	Set `X-Content-Type-Options: nosniff`
5	Missing Referrer-Policy	Low	Set `Referrer-Policy: strict-origin-when-cross-origin`
6	Missing Permissions-Policy	Info–Low	Restrict unused browser features
7	TLS certificate expiry monitoring	Info	Ensure auto-renewal + alerts

Evidence Highlights

• HTTP status: `HTTP/2 200`
• Security headers missing: HSTS, CSP, XFO, nosniff, Referrer-Policy, Permissions-Policy
• TLS issuer: Cloudflare TLS Issuing ECC CA 3
• TLS validity window: Dec 16 2025 → Mar 16 2026

Disclaimer

This assessment is limited to non-intrusive checks and is not a comprehensive penetration test.