BCDRPulse

Automated Security Assessment

example.com

Scan requested Sat, 14 Nov 2026 09:00:00 GMT

B

88 / 100

2 failing · 1 warnings · 24 passing

Automated assessment — not a penetration test.

AI ANALYSIS

Summary: example.com has solid fundamentals and earns a B (88/100). HTTPS is enforced, nothing sensitive is exposed, and email spoofing protection is in place. Three low-severity hardening items keep it from an A.

Top priorities: 1. Tighten the Content-Security-Policy: remove unsafe-inline and unsafe-eval and move to a nonce- or hash-based policy. 2. Add a Cross-Origin-Opener-Policy header (same-origin is the usual value). 3. Add a Cross-Origin-Resource-Policy header (same-origin for a site that serves only its own pages).

Why it matters: a Content-Security-Policy without unsafe-inline is the main defence against cross-site scripting, where injected script can read what a signed-in visitor sees. The two cross-origin headers keep other sites from reaching into your pages and resources.

TRANSPORT

PASS **HTTPS reachable**
The site responded successfully over HTTPS.

PASS **HTTP to HTTPS redirect**
Plain HTTP requests are redirected to HTTPS.

INFO **Deep TLS / certificate analysis**
Certificate expiry, chain validation, cipher-suite strength, and TLS protocol-version analysis require deep inspection available on the Business tier. This automated scan verifies HTTPS works and is enforced, but does not yet inspect the certificate itself.

SECURITY HEADERS

PASS **HTTP Strict Transport Security (HSTS)**
Present: HTTP Strict Transport Security (HSTS) is configured.

PASS **Content Security Policy (CSP)**
Present: Content Security Policy (CSP) is configured.

PASS **Clickjacking protection (X-Frame-Options)**
Present: Clickjacking protection (X-Frame-Options) is configured.

PASS **MIME-sniffing protection (X-Content-Type-Options)**
Present: MIME-sniffing protection (X-Content-Type-Options) is configured.

PASS **Referrer Policy**
Present: Referrer Policy is configured.

PASS **Permissions Policy**
Present: Permissions Policy is configured.

FAIL **Cross-Origin-Opener-Policy (COOP)** LOW
No Cross-Origin-Opener-Policy. COOP isolates your page from cross-origin windows, mitigating some side-channel and tab-nabbing attacks.

FAIL **Cross-Origin-Resource-Policy (CORP)** LOW
No Cross-Origin-Resource-Policy. CORP limits which origins can embed your resources, reducing cross-origin leaks.

WARN **CSP strength** LOW
Your CSP allows unsafe-inline and unsafe-eval, which significantly weakens its XSS protection. Move to a nonce- or hash-based policy and remove these.

INFORMATION DISCLOSURE

PASS **Server version disclosure**
No server version is exposed in the Server header.

PASS **Technology disclosure (X-Powered-By)**
No X-Powered-By header is exposed.

COOKIES

PASS **Cookie security flags**
Cookies are set with Secure, HttpOnly, and SameSite flags.

EXPOSED FILES

PASS **Exposed Git repository (.git/config)**
/.git/config is not publicly accessible.

PASS **Exposed Git repository (.git/HEAD)**
/.git/HEAD is not publicly accessible.

PASS **Exposed environment file (.env)**
/.env is not publicly accessible.

PASS **Exposed SVN metadata (.svn)**
/.svn/entries is not publicly accessible.

PASS **Exposed WordPress config backup**
/wp-config.php.bak is not publicly accessible.

PASS **Exposed .DS_Store (directory listing leak)**
/.DS_Store is not publicly accessible.

PASS **Exposed phpinfo()**
/phpinfo.php is not publicly accessible.

PASS **Exposed Apache server-status**
/server-status is not publicly accessible.

PASS **Exposed Spring Boot Actuator**
/actuator is not publicly accessible.

PASS **Exposed API docs (Swagger UI)**

/swagger-ui.html is not publicly accessible.

BEST PRACTICES

PASS **Security contact (security.txt)**

A /.well-known/security.txt is published, giving researchers a way to report issues.

EMAIL & DNS

PASS **SPF record**

A strict SPF record (-all) is published, helping prevent email spoofing.

PASS **DMARC record**

A DMARC record with p=reject is published - the strongest protection against spoofing.

INFO **DKIM record**

No DKIM record found on common selectors. DKIM signs your outbound mail; if you send email, configure it (the selector name varies by provider, so this check may miss custom ones).

INFO **CAA record**

No CAA record found. Adding one limits which CAs may issue certificates for your domain, reducing the risk of fraudulent certificates.

INFO **Mail servers (MX)**

No MX records found. This domain does not appear to receive email, which is fine for a web-only property.

INFO **DNSSEC**

DNSSEC does not appear to be enabled. It cryptographically signs your DNS records so resolvers can detect tampering - consider enabling it at your DNS provider.