Scan Report for example.com

Red Bridge Cyber · Generated 10 August 2026, 8:01 am UTC

—	A+	A+	F	F
EMAIL	SPEED	DOMAIN	VISIBILITY	SECURITY

6 high, 5 medium, 11 low, 4 info

Executive Summary

Example.com scores well on speed and domain configuration, but has serious gaps in security and search visibility that put the business at risk. On the security side, the site does not automatically redirect visitors from the unsecured version (HTTP) to the encrypted one (HTTPS), and it is missing two important browser-level protections — HSTS and a Content Security Policy — that help prevent data interception and malicious code injection. The domain also lacks CAA records, meaning any certificate authority in the world could technically issue an SSL certificate for your site without your knowledge. Visibility received a failing grade, though the details suggest this stems from the absence of a sitemap or indexing signals rather than the site being actively blocked, and addressing the security issues should be the immediate priority.

What to do next

Severity	Area	Finding	Suggested fix
P1	Visibility	HTTP redirects to HTTPS	http:// did not redirect to https (status 200).
HIGH	Security	Port 80 does not redirect to HTTPS	Redirect port 80 to HTTPS
HIGH	Security	HSTS header missing	Send a Strict-Transport-Security header
HIGH	Security	Content-Security-Policy missing	Send a Content-Security-Policy header
HIGH	Security	TLS 1.0 still enabled	Disable TLS 1.0 on the server
HIGH	Security	TLS 1.1 still enabled	Disable TLS 1.1 on the server
P2	Visibility	robots.txt present	robots.txt missing or empty (status 404).
P2	Visibility	XML sitemap present	No reachable sitemap (checked https://example.com/sitemap.xml, status 404).
P2	Visibility	HSTS header present	HSTS header missing.
P2	Visibility	Content-Security-Policy header present	Content-Security-Policy missing.
P2	Visibility	Content present in raw HTML	Raw HTML near-empty (21 words) — content likely requires JavaScript.

Severity	Area	Finding	Suggested fix
LOW	Domain	No CAA records (any CA can issue certificates)	Publish CAA records (Cloudflare-fronted variant)

10 further lower-severity item(s) appear in Detailed Findings below.

- Add HSTS header and Content-Security-Policy to enforce secure connections and protect against injection attacks.
- Configure port 80 to redirect all HTTP traffic to HTTPS immediately.
- Add CAA DNS records to restrict which certificate authorities can issue SSL certificates for the domain.

How you compare

Recent trend

Needs at least two snapshots — a trend appears once this domain has been scanned on more than one day.

Posture Baseline — SMB cohort

Category	Email	Speed	Domain	Visibility	Security
example.com	—	A+	A+	F	F
Baseline (SMB)	C	D	E	A+	F
Comparison	—	▲ better	▲ better	▼ worse	= same

Baseline = median grade for the selected industry cohort from the Posture Research programme. Visibility is currently benchmarked for SMB only.

Detailed Findings

Email —

No detailed scan data available for this type.

Speed

A+

MOBILE

Performance	100
Accessibility	96
Best practices	96
SEO	80

Core Web Vitals: LCP 755ms, INP 16ms, CLS 0.0, FCP 755ms, TBT 0ms, TTFB 1ms, Speed Index 755ms

DESKTOP

Performance	100
Accessibility	96
Best practices	96
SEO	80

Core Web Vitals: LCP 235ms, INP 16ms, CLS 0.0, FCP 235ms, TBT 0ms, Speed Index 235ms

Domain

A+

A records	104.20.23.154, 172.66.147.243
IPv6 (AAAA)	2606:4700:10::6814:179a, 2606:4700:10::ac42:93f3
MX	(pri 0)
Nameservers	elliott.ns.cloudflare.com, hera.ns.cloudflare.com
Mail provider	other
NS provider	cloudflare

EMAIL AUTHENTICATION

SPF	**Yes** — -all, 0 lookups
SPF record	`v=spf1 -all`
DMARC	**Yes** — policy **reject**, pct 100
DKIM selectors	google, selector1, selector2, default, dkim, mail, k1, key1, key2, s1, s2, mxvault, smtpapi, mandrill, pic, everlytickey1, everlytickey2, dkim1, pm
MTA-STS	**No**
TLS-RPT	**No**
BIMI	**No**

DNS SECURITY

DNSSEC	**Yes**
CAA	**No**

FINDINGS

LOW **No CAA records (any CA can issue certificates)** Fix: Publish CAA records (Cloudflare-fronted variant)

Visibility

F

CATEGORY SCORES

Structured Data	0/100 (fail)
Indexability	50/100 (fail)
Crawlability	50/100 (fail)
Url Structure	100/100 (pass)
Core Web Vitals	100/100 (pass)
Javascript Rendering	0/100 (fail)
Security	25/100 (fail)
Mobile	100/100 (pass)

ISSUES

- P1 **HTTP redirects to HTTPS** — http:// did not redirect to https (status 200).
- P2 **robots.txt present** — robots.txt missing or empty (status 404).
- P2 **XML sitemap present** — No reachable sitemap (checked https://example.com/sitemap.xml, status 404).
- P2 **HSTS header present** — HSTS header missing.
- P2 **Content-Security-Policy header present** — Content-Security-Policy missing.
- P2 **Content present in raw HTML** — Raw HTML near-empty (21 words) — content likely requires JavaScript.
- P3 **Canonical tag present** — No rel=canonical tag.
- P3 **Sufficient content** — 21 visible words. Below the 300-word thin-content threshold.
- P3 **Clickjacking protection present** — No X-Frame-Options or CSP frame-ancestors.
- P3 **X-Content-Type-Options: nosniff present** — X-Content-Type-Options: nosniff missing.
- P3 **Referrer-Policy header present** — Referrer-Policy missing.
- P3 **JSON-LD present** — No JSON-LD blocks found.

OPPORTUNITIES

- INFO **AI-crawler rules present** — No AI-crawler-specific rules in robots.txt.
- INFO **SPA detection** — SPA shell detected: False.

Security

F

HTTPS reachable	Yes
TLS versions	TLSv1.3, TLSv1.1, TLSv1.2, TLSv1.0
Certificate issuer	SSL Corporation
Cert expires	2026-10-27T22:17:21+00:00 (78 days)
HSTS	No
CSP	No

WELL-KNOWN FILES

/sitemap.xml: No
/.well-known/security.txt: No
/robots.txt: No
/favicon.ico: No
/humans.txt: No
/.well-known/change-password: No

FINDINGS

HIGH **Port 80 does not redirect to HTTPS** — http://example.com/ returned status 200 Fix: Redirect port 80 to HTTPS
HIGH **HSTS header missing** Fix: Send a Strict-Transport-Security header
HIGH **Content-Security-Policy missing** Fix: Send a Content-Security-Policy header
HIGH **TLS 1.0 still enabled** Fix: Disable TLS 1.0 on the server
HIGH **TLS 1.1 still enabled** Fix: Disable TLS 1.1 on the server
LOW **X-Content-Type-Options not 'nosniff'** Fix: Send `X-Content-Type-Options: nosniff`
LOW **Referrer-Policy missing** Fix: Send a `Referrer-Policy` header
LOW **Permissions-Policy missing** Fix: Send a `Permissions-Policy` header
LOW **No /.well-known/security.txt** Fix: Publish `/.well-known/security.txt`
INFO **Certificate is CT-logged (2 embedded SCTs)**
INFO **OCSP stapling enabled (status: good)**
INFO **TLS Extended Master Secret supported** — TLS 1.2 ServerHello echoed extended_master_secret
INFO **No /.well-known/change-password redirect** — RFC 8615 / WICG — lets password managers jump straight to your change-password page. One redirect rule on the server. Fix: Add a `/.well-known/change-password` redirect

About this report

Target	example.com
Assessed as	Full domain
Categories scanned	Email, Speed, Domain, Visibility, Security

Snapshots covered	1 daily snapshot(s), 2026-08-10 to 2026-08-10
Baseline cohort	SMB

Grades are derived per category from the checks that category runs: each finding carries a penalty, the penalties are subtracted from 100, and the resulting score maps to a letter. A+ is the top band and F the lowest. Category scores are not averaged into a single overall grade, because a serious email problem and a slow page are not interchangeable.