Recordscan Security Report

DNS, TLS, and HTTP Response Header Audit

Assessment overview

Needs attention

15 total findings across DNS, TLS, and HTTP. 15 are critical, high, or medium severity. 12 HTTP security header checks failed. Legacy TLS versions are enabled: TLS1.0, TLS1.1

In good shape

4 of 16 HTTP header checks passed. Certificate verified; about 75 days until expiry. DNS has 2 nameservers (redundancy OK).

Priority actions

1. Disable TLS 1.0/1.1; prefer TLS 1.2+ and TLS 1.3.
2. Deploy a strict CSP without unsafe-inline/unsafe-eval unless strictly required.
3. Publish CAA limiting issuance to CAs you use; set issuewild if applicable.

Executive summary

Findings	DNS	TLS	HTTP	HTTP OK	TLS grade	Proto	Cert
15	1	2	12	4/16	C	60	100

By severity: high=2, medium=13

DNS records (apex)

Record	Value
A	172.66.147.243 | 104.20.23.154
AAAA	2606:4700:8395:72db:f20c:0:ef6b:ff98
NS	hera.ns.cloudflare.com | elliott.ns.cloudflare.com
MX	0
TXT	_k2n1y4vw3qtb4skdx9e7dxt97qrmmq9 | v=spf1 -all
SOA	elliott.ns.cloudflare.com dns.cloudflare.com
DMARC	v=DMARC1;p=reject;sp=reject;adkim=s;aspf=s
DKIM_default	v=DKIM1; p=

DNS findings

Severity	Category	Title	Detail / fix
MEDIUM	dns_vulnerabilities	No CAA records	Any public CA could issue certificates for this domain unless constrained elsewhere. Fix: Publish CAA limiting issuance to CAs you use; set issuewild if applicable.

TLS / SSL summary

Host	Port	Connected	Version	Cipher	Grade	Score
example.com	443	yes	TLS1.3	TLS_AES_128_GCM_SHA256	C	72

Subject CN	Issuer	Not after (UTC)	Days left	Sig alg	Verified	SAN match
example.com	Cloudflare TLS Issuing ECC CA 1	2026-07-01T21:24:46Z	75	ECDSA-SHA256	true	true

SANs: example.com, *.example.com

Weak protocols enabled: TLS1.0, TLS1.1

TLS 1.2 cipher suites accepted

Cipher suite	Protocol	Score	ID
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	TLS1.2	85	49161
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	TLS1.2	85	49162
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS1.2	40	49171
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS1.2	40	49172
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS1.2	100	49195
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS1.2	100	49196
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS1.2	100	49199
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS1.2	100	49200
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS1.2	100	52392
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	TLS1.2	100	52393
TLS_RSA_WITH_AES_128_CBC_SHA	TLS1.2	40	47
TLS_RSA_WITH_AES_256_CBC_SHA	TLS1.2	40	53
TLS_RSA_WITH_AES_128_CBC_SHA256	TLS1.2	40	60
TLS_RSA_WITH_AES_128_GCM_SHA256	TLS1.2	50	156
TLS_RSA_WITH_AES_256_GCM_SHA384	TLS1.2	50	157
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS1.2	50	49187
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS1.2	40	49191

TLS findings

Severity	Category	Title	Detail / fix
HIGH	ssl_protocol	Legacy TLS enabled: TLS1.0	Server negotiates deprecated protocol versions. Fix: Disable TLS 1.0/1.1; prefer TLS 1.2+ and TLS 1.3.
HIGH	ssl_protocol	Legacy TLS enabled: TLS1.1	Server negotiates deprecated protocol versions. Fix: Disable TLS 1.0/1.1; prefer TLS 1.2+ and TLS 1.3.

HTTP security headers

Base URL	Status	Final URL	Error
https://example.com	200	https://example.com	-

HTTP header checks

Result	Check	Detail
FAIL	Strict-Transport-Security	header missing
FAIL	X-Frame-Options	header missing
FAIL	X-Content-Type-Options	expected nosniff
FAIL	Content-Security-Policy	header missing
FAIL	X-Permitted-Cross-Domain-Policies	expected none
FAIL	Referrer-Policy	expected no-referrer
FAIL	Cross-Origin-Embedder-Policy	expected require-corp
FAIL	Cross-Origin-Opener-Policy	expected same-origin
FAIL	Cross-Origin-Resource-Policy	expected same-origin
FAIL	Permissions-Policy	header missing
FAIL	Cache-Control	expected no-store, max-age=0
FAIL	X-DNS-Prefetch-Control	expected off
PASS	Feature-Policy (should not exist)	
PASS	Public-Key-Pins (should not exist)	
PASS	Expect-CT (should not exist)	
PASS	X-XSS-Protection (should not exist)	
SKIP	Clear-Site-Data	provide --logout-path to test logout response

HTTP findings

Severity	Category	Title	Detail / fix
MEDIUM	http_headers	HTTP header check failed: Strict-Transport-Security	header missing Fix: Set Strict-Transport-Security with long max-age, includeSubDomains, and preload if appropriate.
MEDIUM	http_headers	HTTP header check failed: X-Frame-Options	header missing Fix: Review OWASP Secure Headers guidance and align with your application needs.
MEDIUM	http_headers	HTTP header check failed: X-Content-Type-Options	expected nosniff Fix: Review OWASP Secure Headers guidance and align with your application needs.
MEDIUM	http_headers	HTTP header check failed: Content-Security-Policy	header missing Fix: Deploy a strict CSP without unsafe-inline/unsafe-eval unless strictly required.
MEDIUM	http_headers	HTTP header check failed: X-Permitted-Cross-Domain-Policies	expected none Fix: Review OWASP Secure Headers guidance and align with your application needs.
MEDIUM	http_headers	HTTP header check failed: Referrer-Policy	expected no-referrer Fix: Review OWASP Secure Headers guidance and align with your application needs.

MEDIUM	http_headers	HTTP header check failed: Cross-Origin-Embedder-Policy	expected require-corp Fix: Review OWASP Secure Headers guidance and align with your application needs.
MEDIUM	http_headers	HTTP header check failed: Cross-Origin-Opener-Policy	expected same-origin Fix: Review OWASP Secure Headers guidance and align with your application needs.
MEDIUM	http_headers	HTTP header check failed: Cross-Origin-Resource-Policy	expected same-origin Fix: Review OWASP Secure Headers guidance and align with your application needs.
MEDIUM	http_headers	HTTP header check failed: Permissions-Policy	header missing Fix: Send Permissions-Policy to disable sensitive features by default.
MEDIUM	http_headers	HTTP header check failed: Cache-Control	expected no-store, max-age=0 Fix: Review OWASP Secure Headers guidance and align with your application needs.
MEDIUM	http_headers	HTTP header check failed: X-DNS-Prefetch-Control	expected off Fix: Review OWASP Secure Headers guidance and align with your application needs.