> warden

scanning your app for risk · by veritai

OVERALL SECURITY GRADE

HEALTH 78 / 100 · HARDENING RECOMMENDED

Security Assessment

your-site.com

Prepared 1 September 2026

DEEP SCAN · ACTIVE TESTING

0 Critical	**0** High	**5** Medium	**1** Low

SECURITY ASSESSMENT REPORT

your-site.com

Version 1 · Generated 01 Sep 2026, 09:15 · Profile: Deep Scan

GRADE	HEALTH	RISK	CHECKS RUN	OPEN FINDINGS
C+	78/100	Hardening Recommended	45	6

Priority roadmap

P1 — Immediate security risk

FINDING	SEVERITY	RESPONSIBLE	AFFECTED
No Content-Security-Policy header	Medium	Developer / server admin	https://your-site.com/
Recommended action: Add a Content-Security-Policy. Start in Content-Security-Policy-Report-Only mode to find violations, then enforce.			

P2 — Important hardening

FINDING	SEVERITY	RESPONSIBLE	AFFECTED
TLS certificate expires within 14 days	Medium	Server / hosting admin	https://your-site.com/
Recommended action: Use a valid, current certificate and disable TLS 1.0/1.1 and weak ciphers.			
No SPF record published for the domain	Medium	DNS / email admin	https://your-site.com/
Recommended action: Publish an SPF TXT record listing authorised senders, ending in a policy (~all or -all).			
X-Frame-Options missing	Medium	Developer / server admin	https://your-site.com/
Recommended action: Set X-Frame-Options: SAMEORIGIN (or a CSP frame-ancestors directive) on all responses.			
A cookie is missing the Secure flag	Medium	Developer / server admin	https://your-site.com/
Recommended action: Set Secure on all cookies so they are only sent over HTTPS.			

P3 — Best-practice improvement

FINDING	SEVERITY	RESPONSIBLE	AFFECTED

No Strict-Transport-Security header	Low	Developer / server admin	https://your-site.com/

Recommended action: Send Strict-Transport-Security: max-age=31536000; includeSubDomains on all HTTPS responses.

What changed since last scan

NEW	REOPENED	FIXED	UNCHANGED
0	0	3	6

Resolved since last scan

High	Cross Site Scripting (Reflected)
Low	X-Content-Type-Options missing
Medium	TLS 1.0 is enabled

Category scores

14 of 16 categories assessed this scan.

Category	Score	Scored	Trend
Network Security	**100**/100	0	–
DNS Health	**100**/100	0	–
Patching / Vulnerability Intelligence	**97**/100	1	–
Endpoint Exposure	**100**/100	0	–
Application Security	**100**/100	0	▲ 12
API Security	**100**/100	0	–
TLS / Certificates	**43**/100	1	▼ 48
Web Security Headers	**13**/100	4	▼ 70
Email Security	**20**/100	1	▼ 76
Cloud / Hosting Hygiene	**100**/100	0	–
CDN / WAF Posture	**100**/100	0	–
Information Leakage	**100**/100	0	–
Digital Footprint	**100**/100	0	–
Breach / Threat Intelligence	**100**/100	0	–

Areas not scored this time

Warden did not score these areas this scan — either they do not apply to your site, a check could not complete, or only informational signals came back. They **are left out of** your grade, so they never lower it.

Secure Development Signals	No score for this area this scan
Remediation Progress	No score for this area this scan

Module coverage

MODULE	CHECKS	CATEGORIES ASSESSED
Api	3	API Security (100)
Authn	3	Application Security (100)
Authz	2	Application Security (100)
Cloud	2	Cloud / Hosting Hygiene (100)
Exposure	6	Information Leakage (100) · Digital Footprint (100) · Endpoint Exposure (100)
Headers	8	Web Security Headers (13)
Infrastructure	8	Email Security (20) · DNS Health (100) · CDN / WAF Posture (100) · Breach / Threat Intelligence (100) · Network Security (100)
Tls	7	TLS / Certificates (43)
Web App	6	Application Security (100) · Breach / Threat Intelligence (100)

Scan Depth & Coverage

Depth: Deep Scan (active testing). See the module coverage above for exactly what was assessed.

Warden performs automated, black-box security testing from the outside — it does not have access to the application's source code. Whole classes of issues therefore cannot be exhaustively detected, including business-logic and authorization flaws, many stored/second-order and blind injection paths, vulnerabilities reachable only behind authentication or specific application state, and design-level weaknesses. Absence of findings is not proof that a site is free of vulnerabilities.

A Deep Scan adds active probing (payload injection) but remains automated and black-box; it is not equivalent to a full manual penetration test with source access and human analysis. For high-assurance needs, commission a source-assisted or manual review.

Executive summary

> This report covers the security assessment of your-site.com. It scored 78/100, grade C+ (Hardening Recommended). The open items are lower-severity hardening improvements rather than exploitable vulnerabilities. Since the previous scan the score is up 18 point(s).

Checks overview

Findings by severity

OWASP Top 10 (2021) coverage

A01	Broken Access Control	0
A02	Cryptographic Failures	1
A03	Injection	0
A04	Insecure Design	0
A05	Security Misconfiguration	5
A06	Vulnerable & Outdated Components	0
A07	Identification & Authentication Failures	0
A08	Software & Data Integrity Failures	0
A09	Security Logging & Monitoring Failures	0
A10	Server-Side Request Forgery	0

Top findings by business risk

FINDING	SEVERITY	PRIORITY	WHY IT MATTERS	AFFECTED
TLS certificate expires within 14 days	Medium	P2	Weak TLS can allow interception or downgrade of encrypted traffic.	https://your-site.com/
Next action: Use a valid, current certificate and disable TLS 1.0/1.1 and weak ciphers.				
No Content-Security-Policy header	Medium	P1	CSP is a strong mitigation against cross-site scripting and data injection; without it, an injected script runs unchecked.	https://your-site.com/
Next action: Add a Content-Security-Policy. Start in Content-Security-Policy-Report-Only mode to find violations, then enforce.				

No SPF record published for the domain	Medium	P2	Without SPF, attackers can more easily spoof email from your domain.	https://your-site.com/
Next action: Publish an SPF TXT record listing authorised senders, ending in a policy (~all or -all).				
X-Frame-Options missing	Medium	P2	Allows clickjacking — an attacker overlays your UI inside a hidden frame to trick users into actions.	https://your-site.com/
Next action: Set X-Frame-Options: SAMEORIGIN (or a CSP frame-ancestors directive) on all responses.				
A cookie is missing the Secure flag	Medium	P2	A network attacker on HTTP can capture the cookie.	https://your-site.com/
Next action: Set Secure on all cookies so they are only sent over HTTPS.				
No Strict-Transport-Security header	Low	P3	Visitors can be downgraded to HTTP and exposed to man-in-the-middle interception.	https://your-site.com/
Next action: Send Strict-Transport-Security: max-age=31536000; includeSubDomains on all HTTPS responses.				

Findings by CWE

CWE-319	No Strict-Transport-Security header	1
CWE-326	TLS certificate expires within 14 days	1
CWE-693	No Content-Security-Policy header	1
CWE-290	No SPF record published for the domain	1
CWE-1021	X-Frame-Options missing	1
CWE-614	A cookie is missing the Secure flag	1

Compliance mapping

Open findings mapped to the controls they most likely relate to. This compliance mapping is indicative — it links findings to the controls they most likely relate to, as an aid to remediation and scoping. It is not a certified audit, a formal gap assessment, or a statement of compliance.

PCI DSS 4.0	
2.2.1	5 open findings
6.4.1	5 open findings
4.2.1	1 open finding

PCI DSS 4.0	
3.5.1	1 open finding

ISO/IEC 27001 2022 (ANNEX A)	
A.8.9	5 open findings
A.8.24	1 open finding

SOC 2 TRUST SERVICES CRITERIA	
CC6.1	6 open findings
CC7.1	5 open findings
CC6.7	1 open finding

CYBER ESSENTIALS	
Secure configuration	6 open findings

OWASP ASVS 4.0.3	
V14	5 open findings
V6	1 open finding
V9	1 open finding

Module narratives

Api

The Api module ran 3 checks: 3 passed. It scored 100/100. No failures were found.

Authn

The Authn module ran 3 checks: 3 passed. It scored 100/100. No failures were found.

Authz

The Authz module ran 2 checks: 2 passed. It scored 100/100. No failures were found.

Cloud

The Cloud module ran 2 checks: 2 passed. It scored 100/100. No failures were found.

Exposure

The Exposure module ran 6 checks: 6 passed. No failures were found.

Headers

The Headers module ran 8 checks: 4 passed, 4 failed. It scored 13/100. 4 checks failed and need attention.

Infrastructure

The Infrastructure module ran 8 checks: 7 passed, 1 failed. 1 check failed and need attention.

Tls

The Tls module ran 7 checks: 6 passed, 1 failed. It scored 43/100. 1 check failed and need attention.

Web App

The Web App module ran 6 checks: 5 passed, 1 informational. No failures were found.

Scan confidence: High (100/100)

Full test results

Api

3 passed · 0 failed · 0 warning · 0 info · 0 skipped · 0 error

Passed (3)

Passed	**API CORS policy is restrictive** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**Every documented endpoint requires authentication** **Checked:** With an API token, checks that endpoints require auth, rate-limit, hide sensitive fields, set safe CORS and Cache-Control, and do not advertise unexpected write verbs or upload surfaces; also observes token lifetime and (when configured) object-level authorization. The endpoints are the ones listed on the credential; when none are listed, the API's own published OpenAPI/Swagger document is looked for (the API base path + /openapi.json or /swagger.json, then /openapi.json, /swagger.json, /api/openapi.json, /api-docs, /.well-known/openapi.json; at most 6 GETs) and its parameter-free GET paths are probed, up to 10; failing that, only the base path is checked. An endpoint that answers 404/405/410 with the token as well as without it is recorded as not found (skipped) — never as a rejected token, and never as a passed check. **Why:** Unprotected APIs can leak data or allow actions at scale. **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm

Passed	**No endpoint returned another account's records** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm

Authn

3 passed · 0 failed · 0 warning · 0 info · 0 skipped · 0 error

Passed (3)

Passed	**Login form submits over HTTPS** **Checked:** With credentials, checks that login works over HTTPS with safe session cookies. A sign-in that cannot be completed is recorded as SKIPPED, not failed — it lowers scan confidence (the whole authenticated surface went untested) but never scores against the grade, because the usual cause is a mistyped credential, and the next most common are IP allow-listing, MFA, a captcha or rate limiting, which are the site defending itself. Only a successful login lets the run describe itself as authenticated. Where the site has an area we can name behind the login (a form at /admin/login implies /admin), the sign-in is PROVED by fetching that area and confirming it does not bounce back to the form; the evidence then reads "verified at <path> (HTTP 200)". Some sites offer nothing to probe — a login at the site root, or a back office whose directory index is itself the login page — and those sign-ins are recorded without a "verified at", meaning accepted but unproven. **Why:** Weak login handling can lead to account takeover. **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**Session cookie sets Secure, HttpOnly and SameSite** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm

Passed	**Signed in successfully with the supplied test account** **Checked:** With credentials, checks that login works over HTTPS with safe session cookies. A sign-in that cannot be completed is recorded as SKIPPED, not failed — it lowers scan confidence (the whole authenticated surface went untested) but never scores against the grade, because the usual cause is a mistyped credential, and the next most common are IP allow-listing, MFA, a captcha or rate limiting, which are the site defending itself. Only a successful login lets the run describe itself as authenticated. Where the site has an area we can name behind the login (a form at /admin/login implies /admin), the sign-in is PROVED by fetching that area and confirming it does not bounce back to the form; the evidence then reads "verified at <path> (HTTP 200)". Some sites offer nothing to probe — a login at the site root, or a back office whose directory index is itself the login page — and those sign-ins are recorded without a "verified at", meaning accepted but unproven. **Why:** Weak login handling can lead to account takeover. **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm

Authz

2 passed · 0 failed · 0 warning · 0 info · 0 skipped · 0 error

Passed (2)

Passed	**No administrator-only page was reachable as a standard user** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm

Passed	**Signed-in pages are not reachable while signed out** **Checked:** With credentials, crawls the site while signed in and replays each object URL as a SECOND account of the same credential type and anonymously. A cross-account read is scored ONLY when the first account's identity marker appears in the other's response AND that marker was first proven distinctive on this site: a non-candidate page is fetched as each replaying identity, and a marker that is too short/generic (a bare "test", say) or that already appears there is site furniture, so that leg is reported as NOT TESTED rather than scored. Response similarity is recorded as evidence only and never scores — two correct renders of the same templated page measure about 0.97, so a peer seeing their own equivalent record is indistinguishable from a leak by similarity alone. With one credential it still tests unauthenticated access across the whole authenticated crawl. **Why:** Broken access control is the most common serious web flaw. **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm

Cloud

2 passed · 0 failed · 0 warning · 0 info · 0 skipped · 0 error

Passed (2)

Passed	**Hosting provider identified and responding normally** **Checked:** Checks for publicly-listable object-storage buckets, identifies the hosting/cloud provider, and looks for default server pages and exposed deploy/CI artifacts. **Why:** Cloud and hosting misconfigurations widen the attack surface and can leak data or infrastructure detail. **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**No public cloud storage bucket was found for the domain** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm

Exposure

6 passed · 0 failed · 0 warning · 0 info · 0 skipped · 0 error

Passed (6)

Passed	**.env environment file not exposed** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**.git/config not exposed** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**backup archive not exposed** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**No directory listing at /** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**No exposed environment or configuration files on any discovered host** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**No unauthenticated admin interface was reachable** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm

Headers

4 passed · 4 failed · 0 warning · 0 info · 0 skipped · 0 error

Failed (4)

Failed Medium	**A cookie is missing the Secure flag** **Target:** https://your-site.com/ **Location:** https://your-site.com/ **Fix:** Set Secure on all cookies so they are only sent over HTTPS. confidence: firm
Failed Medium	**Content-Security-Policy missing** **Target:** https://your-site.com/ **Location:** https://your-site.com/ **Fix:** Add a Content-Security-Policy. Start in Content-Security-Policy-Report-Only mode to find violations, then enforce. confidence: firm

Failed **Low**	**HSTS (Strict-Transport-Security) missing** **Target:** https://your-site.com/ **Location:** https://your-site.com/ **Fix:** Send Strict-Transport-Security: max-age=31536000; includeSubDomains on all HTTPS responses. confidence: firm
Failed **Medium**	**X-Frame-Options missing** **Target:** https://your-site.com/ **Location:** https://your-site.com/ **Fix:** Set X-Frame-Options: SAMEORIGIN (or a CSP frame-ancestors directive) on all responses. confidence: firm

Passed (4)

Passed	**Cookies use HttpOnly** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**Permissions-Policy present** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**Referrer-Policy present** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**X-Content-Type-Options present** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm

Infrastructure

7 passed · 1 failed · 0 warning · 0 info · 0 skipped · 0 error

Failed (1)

Failed **Medium**	**No SPF record** **Checked:** Checks the domain's DNS for email-authentication records (SPF, DKIM at common selectors, DMARC). **Why:** Missing SPF/DKIM/DMARC lets attackers spoof email from the domain. **Target:** https://your-site.com/ **Location:** https://your-site.com/ **Fix:** Publish an SPF TXT record listing authorised senders, ending in a policy (~all or -all). confidence: firm

Passed (7)

Passed	**1 A record(s) found** **Checked:** Checks the domain's DNS for email-authentication records (SPF, DKIM at common selectors, DMARC). **Why:** Missing SPF/DKIM/DMARC lets attackers spoof email from the domain. **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**A CDN is serving the site** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**A web application firewall was detected in front of the site** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**DKIM record present (selector: default)** **Checked:** Checks the domain's DNS for email-authentication records (SPF, DKIM at common selectors, DMARC). **Why:** Missing SPF/DKIM/DMARC lets attackers spoof email from the domain. **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**DMARC record present** **Checked:** Checks the domain's DNS for email-authentication records (SPF, DKIM at common selectors, DMARC). **Why:** Missing SPF/DKIM/DMARC lets attackers spoof email from the domain. **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm

Passed	**Not listed or blocked by Google Safe Browsing, Quad9 threat-blocking DNS or Cloudflare malware-blocking DNS as of Tue, Sep 1, 2026 8:15 AM UTC** **Checked:** Checks whether your site is listed on Google Safe Browsing — the list behind the red warning pages in Chrome, Firefox and Safari, covering malware, phishing (social engineering) and unwanted software — by looking up the site root over http and https, the www/apex sibling and a handful of recently crawled pages. It also asks two DNS threat filters, Quad9 and Cloudflare's malware-blocking DNS, whether they block the domain name, because their users cannot reach a blocked site at all. The same check runs daily outside scans, so a new listing is noticed within a day. A listing becomes a Breach / Threat Intelligence finding — Critical for a Google listing, High for a DNS-filter block (only that resolver's users are affected) — that caps the grade until the list clears the domain; you are emailed when your site is listed and again when it clears. Advisory provided by Google Safe Browsing. These checks see your site from the outside. They cannot detect server-side malware, backdoors, or content served only to specific visitors. If you suspect a compromise, run a server-side scan through your hosting provider as well. **Why:** A Safe Browsing listing means browsers block visitors and search traffic collapses; it is the strongest outside evidence that a site has been compromised. **Target:** https://your-site.com/ **Location:** https://your-site.com/ **Evidence:** Advisory provided by Google Safe Browsing confidence: firm
Passed	**Server header discloses version** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm

Tls

6 passed · 1 failed · 0 warning · 0 info · 0 skipped · 0 error

Failed (1)

Failed Medium	**TLS certificate expires within 14 days** **Checked:** Checks the certificate is present, current, and matches the hostname. **Why:** An invalid or expired certificate breaks trust and encryption. **Target:** https://your-site.com/ **Location:** https://your-site.com/ **Fix:** Use a valid, current certificate and disable TLS 1.0/1.1 and weak ciphers. confidence: firm

Passed (6)

Passed	**Certificate chain and TLS robustness checks passed** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**Certificate covers your-site.com** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**No weak TLS ciphers detected** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**TLS 1.0 is disabled** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**TLS certificate not expired for your-site.com** **Checked:** Checks the certificate is present, current, and matches the hostname. **Why:** An invalid or expired certificate breaks trust and encryption. **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**TLS certificate present for your-site.com** **Checked:** Checks the certificate is present, current, and matches the hostname. **Why:** An invalid or expired certificate breaks trust and encryption. **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm

Web App 5 passed · 0 failed · 0 warning · 1 info · 0 skipped · 0 error

Informational (1)

Informational	**ZAP active scan ran authenticated, with the AJAX spider enabled** **Checked:** Intrusive: optional external tool that injects payloads to PROVE web-app flaws (SQL injection, XSS, path traversal). An alert is SCORED only when ZAP proved it — confidence above Low, or Low with concrete evidence (reflected payload, error response); anything less is recorded informational so a guess cannot move the grade, and ZAP's own confidence rides in the evidence string for audit. Off by default, and runs only on a domain with recorded owner authorisation at the active_dast intensity. This is the ZAP leg of the customer-facing Deep Scan (opt-in, per-domain consent, Pro/Agency/Business tiers) — operators can also record consent and launch it from admin. **Why:** Active testing finds real, exploitable vulnerabilities passive scanning cannot — but it sends attack traffic, so it requires explicit consent. **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm

Passed (5)

Passed	**2 third-party ad/analytics script source(s) present in the served HTML** **Target:** https://your-site.com/ **Location:** https://your-site.com/ **Evidence:** googletagmanager.com google-analytics.com confidence: firm
Passed	**CORS policy is restrictive or absent** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
Passed	**No mixed (http://) subresources on the HTTPS page** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm

Passed

No signs of site compromise, defacement or injected scripts

Checked: Reads the homepage and up to N same-site pages from the latest Site Map crawl (Settings → Integrity → "Crawled pages examined per scan") and looks for the visible symptoms of a compromise: scripts from known cryptominer hosts or inline miner loaders; defacement phrases in the title, first heading or visible text; meta-refresh or script redirects to another domain; iframes from other domains that are hidden (1–2 px, display:none, off-screen); spam keyword clusters inside hidden containers or keyword-anchored link farms (a word on a visible page never counts); inline scripts decoding long encoded blobs; and, from the crawl inventory only, links to .php files under wp-content/uploads (never fetched). It then fetches the homepage once more with a Googlebot user agent and compares it for crawler-only spam keywords, a burst of crawler-only external hosts, or a crawler-only off-site redirect — plain content differences never count, and a firewall refusing the spoofed crawler is a skip, not a finding. Signature lists are admin-editable under Settings → Integrity. Everything is read from what the site serves; nothing is executed or uploaded. These checks see your site from the outside. They cannot detect server-side malware, backdoors, or content served only to specific visitors. If you suspect a compromise, run a server-side scan through your hosting provider as well.
Why: These are the marks an attacker leaves once they can write to a site's pages — the stage before, or alongside, an outside blocklist noticing. Cryptominer, defacement and cloaking are Critical; off-site redirect, hidden iframe, hidden spam and PHP under uploads are High; all of those cap the grade. Obfuscated script alone is Low and does not cap.
Target: https://your-site.com/
Location: https://your-site.com/
confidence: firm

Passed

ZAP active scan found no further injection issues

Checked: Intrusive: optional external tool that injects payloads to PROVE web-app flaws (SQL injection, XSS, path traversal). An alert is SCORED only when ZAP proved it — confidence above Low, or Low with concrete evidence (reflected payload, error response); anything less is recorded informational so a guess cannot move the grade, and ZAP's own confidence rides in the evidence string for audit. Off by default, and runs only on a domain with recorded owner authorisation at the active_dast intensity. This is the ZAP leg of the customer-facing Deep Scan (opt-in, per-domain consent, Pro/Agency/Business tiers) — operators can also record consent and launch it from admin.
Why: Active testing finds real, exploitable vulnerabilities passive scanning cannot — but it sends attack traffic, so it requires explicit consent.
Target: https://your-site.com/
Location: https://your-site.com/
confidence: firm

Findings overview

ISSUE	SEVERITY	PRIORITY	OWNER
No Strict-Transport-Security header	Low	P3	Developer / server admin
TLS certificate expires within 14 days	Medium	P2	Server / hosting admin
No Content-Security-Policy header	Medium	P1	Developer / server admin
No SPF record published for the domain	Medium	P2	DNS / email admin
X-Frame-Options missing	Medium	P2	Developer / server admin
A cookie is missing the Secure flag	Medium	P2	Developer / server admin

Detailed findings

Hardening Opportunities

Defence-in-depth improvements — not active vulnerabilities.

No Strict-Transport-Security header

LOW · P3

Headers · Open
CWE-319 OWASP A05
Affected: https://your-site.com/

Priority P3 · Responsible: Developer / server admin · Confirmed · Affects score

The response does not set HTTP Strict-Transport-Security, so browsers may use plain HTTP.

Business risk: Visitors can be downgraded to HTTP and exposed to man-in-the-middle interception.

Technical risk: Without HSTS a network attacker can strip HTTPS on the first visit, intercept credentials, and set cookies before the browser ever sends a secure request.
Remediation: Send Strict-Transport-Security: max-age=31536000; includeSubDomains on all HTTPS responses.
Verify: Fetch the site over HTTPS with `curl -I` and confirm the Strict-Transport-Security header is present with max-age ≥ 31536000; also check that HTTP requests redirect to HTTPS.
Detected by: automated
confidence: firm · first seen 2 Aug 2026 · last seen 1 Sep 2026

TLS certificate expires within 14 days

MEDIUM · P2

Tls · Open
CWE-326 OWASP A02
Affected: https://your-site.com/

Priority P2 · Responsible: Server / hosting admin · Confirmed · Affects score

A TLS configuration weakness was detected.

Business risk: Weak TLS can allow interception or downgrade of encrypted traffic.
Technical risk: A weak or invalid TLS chain enables active MITM, downgrade to exportable ciphers, and forged-certificate impersonation of the host.
Remediation: Use a valid, current certificate and disable TLS 1.0/1.1 and weak ciphers.
Verify: Re-test with `openssl s_client -connect host:443` and an SSL Labs scan; confirm the certificate chain, expiry, and that TLS 1.0/1.1 and weak ciphers are refused.
Detected by: automated
confidence: firm · first seen 2 Aug 2026 · last seen 1 Sep 2026

No Content-Security-Policy header

MEDIUM · P1

Headers · Open
CWE-693 OWASP A05
Affected: https://your-site.com/

Priority P1 · Responsible: Developer / server admin · Confirmed · Affects score

No Content-Security-Policy header is set, so the browser has no allow-list for scripts/resources.

Business risk: CSP is a strong mitigation against cross-site scripting and data injection; without it, an injected script runs unchecked.
Remediation: Add a Content-Security-Policy. Start in Content-Security-Policy-Report-Only mode to find violations, then enforce.
Detected by: automated
confidence: firm · first seen 2 Aug 2026 · last seen 1 Sep 2026

No SPF record published for the domain

MEDIUM · P2

Infrastructure · Open
CWE-290 OWASP A05
Affected: https://your-site.com/

Priority P2 · Responsible: DNS / email admin · Confirmed · Affects score

The domain has no SPF record, so receivers cannot verify which servers may send its mail.

Business risk: Without SPF, attackers can more easily spoof email from your domain.
Remediation: Publish an SPF TXT record listing authorised senders, ending in a policy (~all or -all).
Detected by: automated
confidence: firm · first seen 2 Aug 2026 · last seen 1 Sep 2026

X-Frame-Options missing

MEDIUM · P2

Headers · Open

CWE-1021 OWASP A05

Affected: https://your-site.com/

Priority P2 · Responsible: Developer / server admin · Confirmed · Affects score

No X-Frame-Options (or frame-ancestors) protection, so the page can be framed by other sites.

Business risk: Allows clickjacking — an attacker overlays your UI inside a hidden frame to trick users into actions.
Remediation: Set X-Frame-Options: SAMEORIGIN (or a CSP frame-ancestors directive) on all responses.
Detected by: automated

confidence: firm · first seen 2 Aug 2026 · last seen 1 Sep 2026

A cookie is missing the Secure flag

MEDIUM · P2

Headers · Open

CWE-614 OWASP A05

Affected: https://your-site.com/

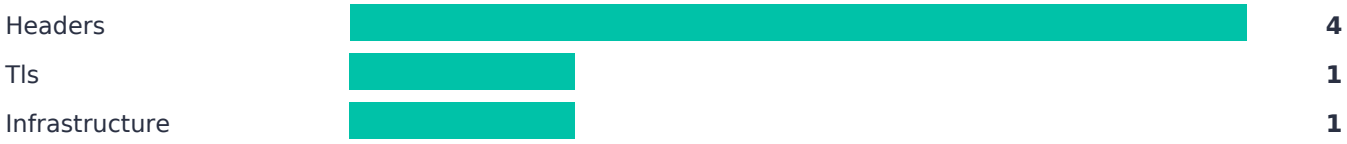
Priority P2 · Responsible: Developer / server admin · Confirmed · Affects score

A cookie is missing the Secure attribute, so it can be sent over plain HTTP.

Business risk: A network attacker on HTTP can capture the cookie.
Remediation: Set Secure on all cookies so they are only sent over HTTPS.
Detected by: automated

confidence: firm · first seen 2 Aug 2026 · last seen 1 Sep 2026

Findings by category



Vulnerability Intelligence, Blocklists & End-of-Life

Known security advisories (CVE / GHSA, including CISA Known-Exploited), end-of-life components, and any security-blocklist listing or DNS-filter block currently affecting this domain. Entries rated Low or higher feed the overall security grade; informational entries are shown for awareness. Snapshot taken at report generation.

ADVISORY	AFFECTED COMPONENT	SEVERITY	KEV	EPSS	CVSS BASE
CVE-2023-45143	undici 5.26.2	Low	—	0.1%	3.5
Priority P3. Upgrade undici to 5.26.3 or later.					

Remediation roadmap

Quick wins

SEVERITY	ACTION
Medium	**TLS certificate expires within 14 days** · https://your-site.com/ Use a valid, current certificate and disable TLS 1.0/1.1 and weak ciphers.

Medium	**No Content-Security-Policy header** · https://your-site.com/ Add a Content-Security-Policy. Start in Content-Security-Policy-Report-Only mode to find violations, then enforce.
Medium	**No SPF record published for the domain** · https://your-site.com/ Publish an SPF TXT record listing authorised senders, ending in a policy (~all or -all).
Medium	**X-Frame-Options missing** · https://your-site.com/ Set X-Frame-Options: SAMEORIGIN (or a CSP frame-ancestors directive) on all responses.
Medium	**A cookie is missing the Secure flag** · https://your-site.com/ Set Secure on all cookies so they are only sent over HTTPS.
Low	**No Strict-Transport-Security header** · https://your-site.com/ Send Strict-Transport-Security: max-age=31536000; includeSubDomains on all HTTPS responses.

Long-term recommendations

SEVERITY	ACTION
Info	**Apply HTTP security headers globally (HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy) at the web server or edge.** Apply HTTP security headers globally (HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy) at the web server or edge.
Info	**Implement SPF, DKIM and DMARC for the domain to prevent email spoofing.** Implement SPF, DKIM and DMARC for the domain to prevent email spoofing.
Info	**Set up recurring scans with retest comparison so regressions are caught and progress is tracked over time.** Set up recurring scans with retest comparison so regressions are caught and progress is tracked over time.

Evidence appendix

SOURCE	EVIDENCE

No Content-Security-Policy header
headers.csp
Confidence: firm
Detected: 1 Sep 2026, 09:15
	Response headers with no Content-Security-Policy
	`HTTP/1.1 200 OK`
	`strict-transport-security: max-age=2592000`
	`x-content-type-options: nosniff`

Technical metadata

PROFILE	Deep Scan
INTENSITY	Active Dast
VERIFICATION	Verified

TIMELINE	queued 1 Sep 2026, 09:06 · started 1 Sep 2026, 09:07 · finished 1 Sep 2026, 09:15

How to read this report

The health score starts at 100. Each open finding subtracts points based on its severity, weighted by confidence and exposure — so every finding moves the number and two sites with different issues get different scores. The score reflects what is currently open and does not drift up on its own between scans: an unresolved finding is never discounted just because the last scan is older. The final score (0–100) maps to a letter grade on a thirteen-band ladder (A+ down to F, with + and − steps). The letter grade is shown as a disc on the report cover, alongside the health score and risk level; the pages that follow break the result down section by section.

Grade	Score is at least
A+	97
A	93
A-	90
B+	87
B	83
B-	80
C+	77
C	73
C-	70
D	60
E	50
F	0

Each finding carries a severity, shown throughout the report as a coloured pill:

Severity	Meaning
Critical	A serious flaw that is likely being or could easily be exploited. Fix immediately.
High	An important weakness that could lead to compromise. Fix as a priority.
Medium	A weakness that increases risk and should be scheduled for remediation.
Low	A minor issue or hardening opportunity with limited direct impact.
Info	Informational only — context for review, not a vulnerability by itself.

Risk levels: Low / Medium / High / Critical — the worse of the score band and the most serious open finding. **Not scored:** a category Warden did not score this scan (does not apply, a check could not complete, or only informational signals) — it is left out of the grade, so it never lowers it. **Scan confidence:** how much of the scan ran unobstructed (separate from the security grade). Checks that don't apply to this site — no login credentials supplied, no API configured — appear as coverage notes and do not reduce confidence; a Low band means parts of the scan were genuinely blocked and marks the grade provisional. **Grade caps:** an open vulnerability caps the grade by its severity — high caps at D, medium at C-, critical at F — while hardening gaps (missing headers, email records, configuration) lower the score but never cap it. **Catch-all routing:** if the site answers every address, exposed-file and credential checks cannot run reliably, so the grade is capped at C- and marked provisional until it is verified by hand.

Findings are listed twice: a compact **overview table** (issue, severity, priority, owner) followed by a **detailed card** per finding with evidence and remediation. Priority is colour-coded P1 (most urgent) to P4:

Priority level	Meaning

P1	Immediate security risk	Critical or high severity — address immediately.
P2	Important hardening	Medium severity (or high with lower confidence) — address in the next maintenance cycle.
P3	Best-practice improvement	Low severity — schedule as a best-practice improvement.
P4	Informational / monitor	Informational — monitor and review periodically.

Responsible party: the team or role best placed to implement the fix — Developer, Server / hosting admin, DNS / email admin, or Hosting provider. Derived from the finding category and check type; review with your own team structure.

Detection confidence	Meaning
Confirmed	Verified by direct observation — the check produced unambiguous evidence.
Inferred	Derived from indirect signals — the finding is likely but not directly observed.
Needs manual verification	Automated detection flagged a potential issue; a human tester should confirm before actioning.