> warden

scanning your app for risk · by veritai

OVERALL SECURITY GRADE

HEALTH 84 / 100 · HARDENING RECOMMENDED

Security Assessment

your-site.com

Prepared 1 July 2026

DEEP SCAN · AUTHENTICATED ACTIVE TESTING

0 Critical	**0** High	**3** Medium	**1** Low

SECURITY ASSESSMENT REPORT

your-site.com

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

GRADE	HEALTH	RISK	CHECKS RUN	OPEN FINDINGS
B	84/100	Hardening Recommended	37	4

Priority roadmap

P1 — Immediate security risk

FINDING	SEVERITY	RESPONSIBLE	AFFECTED	RECOMMENDED ACTION
No Content-Security-Policy header	Medium	Developer / server admin		Add a Content-Security-Policy header. Start in report-only mode to find breakages, then enforce a policy that names your...

P2 — Important hardening

FINDING	SEVERITY	RESPONSIBLE	AFFECTED	RECOMMENDED ACTION
TLS certificate expires within 14 days	Medium	Server / hosting admin	https://your-site.com	Renew the certificate and automate renewal (for example with certbot or your host's managed TLS) so it cannot lapse agai...
No SPF record published for the domain	Medium	DNS / email admin		Publish an SPF TXT record listing every authorised sending service, ending in a policy (~all while testing, -all once co...

P3 — Best-practice improvement

FINDING	SEVERITY	RESPONSIBLE	AFFECTED	RECOMMENDED ACTION
No Strict-Transport-Security header	Low	Developer / server admin		Send Strict-Transport-Security: max-age=31536000; includeSubDomains on every HTTPS response once you have confirmed all...

What changed since last scan

NEW	REOPENED	FIXED	UNCHANGED
0	0	3	4

Resolved since last scan

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

Category scores

9 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	–
Application Security	**100**/100	0	▲ 12
API Security	**100**/100	0	–
TLS / Certificates	**43**/100	1	▼ 48
Web Security Headers	**65**/100	2	▼ 27
Email Security	**20**/100	1	▼ 76
Information Leakage	**100**/100	0	–

Not assessed this scan

Warden could not score these areas this scan (checks were skipped, a scanner errored, or only informational signals were seen). They **do not count for or against** your grade.

Endpoint Exposure	Not assessed in this scan
Cloud / Hosting Hygiene	Not assessed in this scan
CDN / WAF Posture	Not assessed in this scan
Digital Footprint	Not assessed in this scan
Breach / Threat Intelligence	Not assessed in this scan
Secure Development Signals	Not assessed in this scan
Remediation Progress	Not assessed in this scan

Module coverage

MODULE	CHECKS	CATEGORIES ASSESSED
Api	3	API Security (100)

Authn	3	Application Security (100)
Authz	2	Application Security (100)
Exposure	4	Information Leakage (100)
Headers	8	Web Security Headers (65)
Infrastructure	5	Email Security (20) · DNS Health (100) · Network Security (100)
Tls	7	TLS / Certificates (43)
Web App	5	Application Security (100)

Scan Depth & Coverage

Depth: Deep Scan (authenticated 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.

How this compares with a manual penetration test

For a specific set of checks, this scan used the same techniques a human tester would: it signed in with a real account, sent live attack payloads to test for SQL injection, cross-site scripting and path traversal, checked whether a standard user could reach administrator-only areas, and examined how your session is issued and protected. For those checks the coverage is comparable to the automated portion of a professional test. What it does not replace is the human half — reasoning about your business rules, chaining several small weaknesses into a single attack, abusing multi-step workflows, and judging what an attacker would actually want from your application. Those need a person, and they are often where the most valuable findings come from. Treat this as continuous automated assurance between manual tests, not as a replacement for one.

Executive summary

> This report covers the security assessment of your-site.com. It scored 84/100, grade B (Hardening Recommended). The open items are lower-severity hardening improvements rather than exploitable vulnerabilities. Since the previous scan the score is up 24 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	3
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	NEXT ACTION
TLS certificate expires within 14 days	Medium	P2	If the certificate lapses, every visitor sees a full-page browser security warning and the site is effectively offline until it is renewed.	https://your-site.com	Renew the certificate and automate renewal (for example with certbot or your host's managed TLS) so...
No Content-Security-Policy header	Medium	P1	Without a CSP, a single injected script — from a compromised third-party tag or an XSS flaw — can run unchecked. A CSP is the control that contains the damage when something else goes wrong.		Add a Content-Security-Policy header. Start in report-only mode to find breakages, then enforce a po...

No SPF record published for the domain	Medium	P2	Someone can send email that appears to come from your domain, and most receiving servers have no policy telling them otherwise — a common route into invoice fraud and phishing aimed at your customers.		Publish an SPF TXT record listing every authorised sending service, ending in a policy (~all while t...
No Strict-Transport-Security header	Low	P3	A returning visitor who types the bare domain or follows an old http:// link is exposed to a downgrade attack on an untrusted network before HTTPS ever kicks in.		Send Strict-Transport-Security: max-age=31536000; includeSubDomains on every HTTPS response once you...

Findings by CWE

CWE-324	TLS certificate expires within 14 days	1
CWE-693	No Content-Security-Policy header	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	3 open findings
6.4.1	3 open findings
4.2.1	1 open finding
3.5.1	1 open finding

ISO/IEC 27001 2022 (ANNEX A)	
A.8.9	3 open findings
A.8.24	1 open finding

SOC 2 TRUST SERVICES CRITERIA

CC6.1	4 open findings
CC7.1	3 open findings
CC6.7	1 open finding

CYBER ESSENTIALS	
Secure configuration	4 open findings

OWASP ASVS 4.0.3	
V14	3 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.

Exposure

The Exposure module ran 4 checks: 4 passed. It scored 100/100. No failures were found.

Headers

The Headers module ran 8 checks: 6 passed, 2 failed. It scored 65/100. 2 checks failed and need attention.

Infrastructure

The Infrastructure module ran 5 checks: 4 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 5 checks: 4 passed, 1 informational. It scored 100/100. 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 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. **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. **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. **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

Exposure

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

Passed (4)

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

Headers

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

Failed (2)

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

Passed (6)

Passed	**A cookie is missing the Secure flag** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm
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
Passed	**X-Frame-Options missing** **Target:** https://your-site.com/ **Location:** https://your-site.com/ confidence: firm

Infrastructure

4 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 (4)

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	**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	**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

4 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 (4)

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

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

Detailed findings

Hardening Opportunities

Defence-in-depth improvements — not active vulnerabilities.

No Strict-Transport-Security header

LOW · P3

Headers · Open

OWASP A05

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

The site does not send a Strict-Transport-Security header, so browsers do not remember to use HTTPS-only on a visitor's next visit.

Business risk: A returning visitor who types the bare domain or follows an old http:// link is exposed to a downgrade attack on an untrusted network before HTTPS ever kicks in.
Technical risk: Without HSTS a network attacker can strip HTTPS on the first request of a session, intercepting traffic before any redirect to HTTPS occurs.

Remediation: Send Strict-Transport-Security: max-age=31536000; includeSubDomains on every HTTPS response once you have confirmed all subdomains are HTTPS-only.
Verify: Fetch the site over HTTPS and confirm the Strict-Transport-Security header is present with max-age of at least 31536000.
Detected by: automated
References: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
confidence: firm · first seen 1 Jun 2026 · last seen 1 Jul 2026

TLS certificate expires within 14 days

MEDIUM · P2

Tls · Open
CWE-324 OWASP A02
Affected: https://your-site.com

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

The certificate presented by the site expires within 14 days.

Business risk: If the certificate lapses, every visitor sees a full-page browser security warning and the site is effectively offline until it is renewed.
Technical risk: An expired leaf certificate fails validation in all major browsers and in most API clients.
Remediation: Renew the certificate and automate renewal (for example with certbot or your host's managed TLS) so it cannot lapse again.
Verify: Re-run the scan after renewal and confirm the certificate expiry is more than 14 days out.
Detected by: automated
References: https://letsencrypt.org/docs/
confidence: firm · first seen 1 Jun 2026 · last seen 1 Jul 2026

No Content-Security-Policy header

MEDIUM · P1

Headers · Open
CWE-693 OWASP A05

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

The site does not send a Content-Security-Policy header, so the browser has no instruction limiting where scripts may be loaded from.

Business risk: Without a CSP, a single injected script — from a compromised third-party tag or an XSS flaw — can run unchecked. A CSP is the control that contains the damage when something else goes wrong.
Technical risk: No restriction on script-src, so any injected or third-party script executes with full origin privileges.
Remediation: Add a Content-Security-Policy header. Start in report-only mode to find breakages, then enforce a policy that names your script origins explicitly and avoids unsafe-inline.
Verify: Request any page and confirm a Content-Security-Policy response header is present and does not contain unsafe-inline in script-src.
Detected by: automated
References: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
confidence: firm · first seen 1 Jun 2026 · last seen 1 Jul 2026

No SPF record published for the domain

MEDIUM · P2

Infrastructure · Open
OWASP A05

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

The domain has no SPF record, so mail receivers cannot verify which servers are authorised to send mail on its behalf.

Business risk: Someone can send email that appears to come from your domain, and most receiving servers have no policy telling them otherwise — a common route into invoice fraud and phishing aimed at your customers.
Technical risk: Without an SPF TXT record, receivers fall back to their own default handling of unauthenticated senders, which is inconsistent and frequently permissive.
Remediation: Publish an SPF TXT record listing every authorised sending service, ending in a policy (~all while testing, -all once confirmed).
Verify: Query the domain's TXT records and confirm an SPF record (v=spf1 ...) is present.
Detected by: automated
References: https://datatracker.ietf.org/doc/html/rfc7208
confidence: firm · first seen 1 Jun 2026 · last seen 1 Jul 2026

Findings by category

Vulnerability Intelligence & End-of-Life

Known security advisories (CVE / GHSA, including CISA Known-Exploited) and end-of-life components currently affecting technologies detected on 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 Renew the certificate and automate renewal (for example with certbot or your host's managed TLS) so it cannot lapse again.
Medium	**No Content-Security-Policy header** Add a Content-Security-Policy header. Start in report-only mode to find breakages, then enforce a policy that names your script origins explicitly and avoids unsafe-inline.
Medium	**No SPF record published for the domain** Publish an SPF TXT record listing every authorised sending service, ending in a policy (~all while testing, -all once confirmed).
Low	**No Strict-Transport-Security header** Send Strict-Transport-Security: max-age=31536000; includeSubDomains on every HTTPS response once you have confirmed all subdomains are HTTPS-only.

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 Jul 2026, 09:15
Verify: Request any page and confirm a Content-Security-Policy response header is present and does not contain unsafe-inline in script-src.
	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 Jul 2026, 09:06 · started 1 Jul 2026, 09:07 · finished 1 Jul 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 assessed:** a category Warden could not score this scan (skipped, errored, or only informational signals) — it does not count for or against the grade. **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.