Website Audit Report — SAMPLE

This is a real report, generated on 2026-10-23 by running the same tool battery the $49 Website Audit delivers, against papacasper.com (the seller's own site). Nothing is cherry-picked — the findings include what this site gets wrong. Raw tool output: raw-output/ folder alongside this file.

Site: https://papacasper.com

Date: 2026-10-23

Package: Website Audit ($49) — full battery

Prepared by: William — PapaCasper

Overall Scores

Area — Result

SEO: 82 / 100

Site Health (DNS, SSL, mail): Pass — no issues found

Security: Headers **80 / 100** · Exposed files: **none found**

Speed: 93 / 100 (Google PageSpeed, mobile)

SSL Grade: B (SSL Labs) · certificate valid, 83 days remaining

AI Readiness: 85 / A

Summary

papacasper.com is a healthy site with an unusually strong AI-readiness profile — it scores 85/A where most sites have never been checked at all. The checks found no exposed files, no blacklist listings, no DNS or mail problems, and a fast mobile PageSpeed score of 93. Three things need attention: one affiliate link on the homepage appears to be dead (a revenue problem, not a technicality), the site states no explicit policy for AI crawlers in robots.txt, and the SSL configuration grades B instead of A. All three are fixable in an afternoon.

---

1. SEO Audit

Result: 82 / 100 — Needs attention (minor)

Finding: The fundamentals are in place. Title ("PapaCasper") and meta description ("Links, products, and videos from PapaCasper.") are present, the canonical URL is correct, Open Graph and Twitter card tags are complete, both images on the page have alt text, and the page carries 2 blocks of structured data. robots.txt and sitemap.xml are both present.

Finding: No apple-touch-icon. When an iPhone user saves the site to their home screen, iOS falls back to a low-quality screenshot icon instead of a branded one.

Recommended fix: Add a 180×180 PNG and <link rel="apple-touch-icon" href="/apple-touch-icon.png"> to the page head.

Finding: No web app manifest. The site can't be "installed" as a PWA, and browsers get no name/icon/theme declaration.

Recommended fix: Add a minimal manifest.webmanifest (name, short name, icons, theme/background colors) and link it in the head.

Finding: No theme-color meta tag, so mobile browser chrome doesn't pick up the site's branding.

Recommended fix: Add <meta name="theme-color" content="#0b0f0c"> (or your brand color).

Finding (context, not a defect): The homepage is a link hub — 85 words, one H1, no H2/H3 subheadings, 3 internal and 11 external links. For a links page that's by design; it does mean the page itself has almost no searchable content, so search traffic has to come from other pages on the domain.

2. Site Health (DNS, WHOIS, SSL, Mail Records)

Result: Pass

Finding: The domain is registered with Dynadot, created 2023-04-14, and doesn't expire until **2031-04-14 — 1,634 days of runway**, with transfer lock (clientTransferProhibited) on. There is no expiry risk here for years.

Finding: DNS is healthy. Nameservers are Cloudflare's (henry/kara.ns.cloudflare.com), A and AAAA records resolve through Cloudflare, and mail is handled by the site's own server (MX: mail.papacasper.com). The health check reported zero DNS issues.

Finding: The SSL certificate is valid — issued to papacasper.com (issuer WE1 / Google Trust Services, served via Cloudflare), expiring 2027-01-13, 83 days remaining at audit time. Auto-renewal via Cloudflare makes this a non-issue, but it's verified, not assumed.

Finding (minor): DNSSEC is unsigned. Not a functional problem, but enabling DNSSEC at the registrar/Cloudflare closes a DNS-spoofing gap and is a one-setting change.

3. Broken Links

Result: Needs attention — 1 link to verify by hand

A crawl of the site (3 pages, 9 links checked) flagged 3 links. Two are checker artifacts; one matters:

Finding: The **NordVPN referral link** on the homepage (refer-nordvpn.com/...) returned **404** during the crawl. If it returns 404 for visitors too, this is a dead affiliate link — it's sending your audience to an error page instead of earning commission.

Recommended fix: Click the link in a normal browser. Some affiliate networks block automated checkers, so confirm first; if it 404s for you as well, replace it with a fresh referral URL from your NordVPN affiliate dashboard and re-check.

Finding (artifact): The TikTok profile link returned 403. TikTok blocks automated requests — the link itself is almost certainly fine.

Finding (artifact): A /cdn-cgi/l/email-protection path returned 404. That's Cloudflare's email-obfuscation machinery, not a real page link. Ignore.

4. Security Headers & Exposed Files

Result: Headers 80 / 100 — Needs attention · Exposed files: Pass

Finding: The strong headers are present and correctly set: Strict-Transport-Security (1 year, includes subdomains), X-Frame-Options SAMEORIGIN, X-Content-Type-Options nosniff, X-XSS-Protection. CORS is clean — no wildcard origins, no arbitrary-origin reflection.

Finding: No Content-Security-Policy header. CSP is the main defense-in-depth layer against cross-site scripting and injection — if any script on the page is ever compromised, there's no policy limiting what it can load or where it can send data.

Recommended fix: Add a CSP, starting in report-only mode (Content-Security-Policy-Report-Only) to catch breakage safely, then enforce. This is the single highest-value security fix on the site.

Finding: No Referrer-Policy header. Without one, full page URLs (including any query strings) can leak to third parties when visitors click outbound links — and this site is mostly outbound links.

Recommended fix: Add Referrer-Policy: strict-origin-when-cross-origin (one line in the server config).

Finding (minor): No Permissions-Policy header. Low risk for a links page; add one to switch off browser features the site never uses (camera, microphone, geolocation).

Finding: Exposed files: none. 25 sensitive paths were probed (.env variants, .git, .aws credentials, SSH keys, database dumps, backup archives, phpinfo, .DS_Store, and similar). Zero were reachable. This is the check that finds other people's disasters — yours is clean.

5. Email Deliverability (SPF / DKIM / DMARC)

Result: Pass

Finding: SPF is published and strict: v=spf1 mx a ip4:15.204.209.89 ip6:… -all — the -all hard-fail tells receivers to reject mail that pretends to come from this domain but doesn't come from its servers. It uses only 2 of the 10 permitted DNS lookups, so there's no lookup-limit risk.

Finding: DKIM is published (found under the mail selector, RSA key). Mail from this domain can be cryptographically verified by receivers.

Finding: DMARC is published with a real enforcement policy: p=quarantine, with aggregate reporting to postmaster@papacasper.com and failure reporting on (fo=1). Unauthenticated mail claiming to be from this domain gets sent to spam rather than delivered.

Recommended fix (optional tightening): Once you're confident all legitimate sending sources are covered, step DMARC from quarantine up to reject — the maximum enforcement. Not urgent; quarantine is already a passing grade most domains don't have.

Finding: Blacklists — the mail server's IP is **not listed** on SpamCop or Barracuda. One list, Spamhaus Zen, could not be confirmed either way: Spamhaus refuses queries that arrive via public DNS resolvers, so its answer was "unknown," not "listed" and not "clean." This is stated here exactly as the tool reported it.

Finding: The mail server's reverse DNS (PTR) correctly resolves back to mail.papacasper.com — a small detail receivers check and many self-hosted setups get wrong.

6. Speed & SSL Grade

Result: PageSpeed 93 / 100 (mobile) · SSL Labs grade B

Finding: Google's PageSpeed Insights (mobile) scored the site **93**. Core numbers: First Contentful Paint 2.6s, Largest Contentful Paint 2.6s, Total Blocking Time 0 ms, Cumulative Layout Shift 0, Speed Index 3.2s, Time to Interactive 2.6s. Zero blocking time and zero layout shift are as good as it gets; the only soft spot is the 2.6s paint time, typical for an image-forward page on mobile.

Caveat: Google has no real-user field data for this URL (not enough Chrome traffic in the CrUX dataset), so these are lab numbers — measured, but from a test device rather than your actual visitors.

Finding: The SSL Labs assessment graded the site's TLS configuration **B** (all completed edge endpoints; no warnings flagged). B is a passing, secure grade — your visitors are not at risk — but it's the weakest headline number in this report. On Cloudflare-hosted sites a B is most commonly a capability cap from legacy TLS versions (1.0/1.1) still being enabled for old-device compatibility.

Recommended fix: In the Cloudflare dashboard, set the minimum TLS version to 1.2 (SSL/TLS → Edge Certificates), then re-run the grade. If any audience segment genuinely needs TLS 1.0/1.1, leave it — B is safe; this is polish, not a hole.

7. AI Readiness

Score: 85 / A

Finding: Almost everything AI crawlers and agents look for is present and scoring maximum points: llms.txt exists and is well-formed (has a heading, links, and real content — 25/25), robots.txt is present (10/10), the page has JSON-LD structured data and Open Graph tags (15/15), agent/payment discovery files are live (/.well-known/x402 and /openapi.json — 15/15), a sitemap exists (10/10), and title/meta basics are covered (10/10).

Finding: The one gap, worth the full 15 points it costs: **robots.txt states no explicit policy for any known AI crawler** (0 of 12 tracked agents — GPTBot, ClaudeBot, CCBot, PerplexityBot, and others — are mentioned). Right now your stance toward AI training and AI search crawlers is whatever each crawler defaults to, not a decision you made.

Recommended fix: Decide, per crawler, whether you want to be crawlable (discoverable in AI search answers, but also trainable) or blocked, and write those rules into robots.txt explicitly. For a site whose products are aimed at agents, the natural choice is to explicitly

allow the search/retrieval crawlers — it converts an accident into a policy and takes this section to ~100.

Top 5 Fixes First

Work through these in order — highest impact first.

1. **Verify the NordVPN referral link** — it returned 404 in the crawl. If it's dead for visitors, it's a revenue link earning nothing. Five minutes to check, one paste to fix.
2. **Write an explicit AI-crawler policy into robots.txt** — the only gap in an otherwise perfect AI-readiness profile; it decides whether AI search can find and cite this site.
3. **Add a Content-Security-Policy (report-only first) and a Referrer-Policy header** — closes both warned gaps in an otherwise strong header set; security score 80 → ~95.
4. **Add apple-touch-icon, web app manifest, and theme-color** — the three site-chrome gaps from the SEO audit. Under an hour, all three, and every mobile visitor sees the difference.
5. **Set minimum TLS to 1.2 in Cloudflare and re-grade** — the usual path from SSL Labs B to A. (Runner-up: step DMARC from quarantine to reject once you're sure every legitimate sender is covered.)

Appendix: Raw Findings

Full unedited JSON output from every tool run (2026-10-23) accompanies this sample in the raw-output/ folder:

- domain_report.json — SEO + domain health (WHOIS/DNS) + email deliverability bundle
- seo_audit.json — score 82; issues: apple-touch-icon, manifest, theme-color
- ai_readiness_audit.json — score 85, grade A; issue: no explicit AI-crawler policy
- security_headers_audit.json — score 80; CSP and Referrer-Policy missing; CORS clean
- exposed_files_check.json — 25 paths probed, 0 exposed, 0 inconclusive
- broken_link_check.json — 9 links checked, 3 flagged (see §3 for which are real)
- pagespeed_insights.json — mobile performance 93; FCP/LCP 2.6s; TBT 0 ms; CLS 0
- ssl_cert_check.json — issuer WE1, valid to 2027-01-13, 83 days remaining
- ssl_labs_grade.json — grade B on all completed endpoints, no warnings

End of sample report. This is the exact format, depth, and tone a buyer's report follows — generated from their site's data, with their checkout focus areas answered first in the summary.