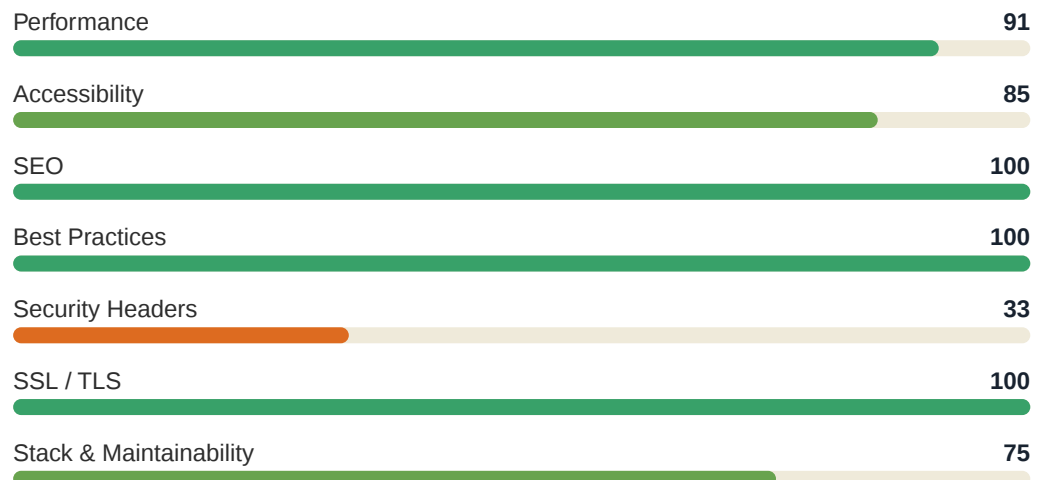




**A WordPress  
Business Site**  
OVERALL GLOSSYDEV  
SCORE



## Consultant's Summary

**A fast, well-built site that's quietly exposed on security — the fixes are straightforward but genuinely urgent.**

The fundamentals here are strong: your site loads quickly, search engines can read it perfectly, and the technical build follows current standards. That's a solid foundation most businesses don't have. The concern is on the security side — several outdated plugins carry known vulnerabilities and some standard protective settings aren't in place, which leaves an otherwise polished site more open to attack than it should be. These are fixable in a focused session, not a rebuild.

- 1 Update the four flagged plugins to their latest versions right away**  
Outdated plugins are the leading cause of WordPress site compromises, and one of yours has nine known vulnerabilities on record — this is your biggest exposure to downtime or a breach.
- 2 Add the missing security headers on the server**  
These are quick, one-time settings that protect against common attacks like clickjacking and force secure connections, closing gaps that currently leave the site more vulnerable.
- 3 Put a routine maintenance process in place for plugins and updates**  
Regular upkeep keeps the site secure over time and protects the strong performance and search standing you've already earned, rather than patching problems after they surface.

## Performance — Core Web Vitals

### Mobile — stress test (simulated slow 4G)

|                          |       |
|--------------------------|-------|
| Largest Contentful Paint | 3.0 s |
| Total Blocking Time      | 0 ms  |
| Cumulative Layout Shift  | 0.000 |

### Desktop — lab test

|                          |        |
|--------------------------|--------|
| Largest Contentful Paint | 957 ms |
| Total Blocking Time      | 0 ms   |
| Cumulative Layout Shift  | 0.002  |

The lab test deliberately simulates a budget phone on a slow connection — a worst-case stress test that exposes bottlenecks, not how long the site takes for a typical visitor (who will see it load several times faster).

What real visitors actually experienced (Chrome data, last 28 days): LCP 4.0 s · INP 63 ms · CLS 0.020 — these real-user numbers are the ground truth.

## What to fix first

- HIGH** **Several security headers are missing**  
The site is missing: HSTS (forces HTTPS); X-Frame-Options (clickjacking protection); X-Content-Type-Options (MIME-sniffing protection); Referrer-Policy (privacy). These are quick server-side wins that harden the site against common attacks.
- GOOD** **Valid HTTPS certificate**  
Secured by Let's Encrypt.

## Additional items worth addressing

The full remaining technical audit — lower-impact items, included so your team or IT department can verify everything found.

### PERFORMANCE · 11

- <sup>a</sup> Render-blocking requests — Est savings of 1,930 ms
- <sup>a</sup> Use efficient cache lifetimes — Est savings of 52 KiB
- <sup>a</sup> Network dependency tree
- <sup>a</sup> Font display — Est savings of 30 ms
- <sup>a</sup> Forced reflow
- <sup>a</sup> LCP request discovery
- <sup>a</sup> First Contentful Paint — 3.0 s
- <sup>a</sup> Reduce unused CSS — Est savings of 38 KiB
- <sup>a</sup> Improve image delivery — Est savings of 451 KiB
- <sup>a</sup> Speed Index — 4.4 s
- <sup>a</sup> Largest Contentful Paint — 3.0 s

### ACCESSIBILITY · 4

- <sup>a</sup> Background and foreground colors do not have a sufficient contrast ratio.
- <sup>a</sup> Links do not have a discernible name
- <sup>a</sup> Heading elements are not in a sequentially-descending order
- <sup>a</sup> Form elements do not have associated labels

## Recent plugin vulnerabilities

These WordPress plugins have had security vulnerabilities disclosed recently. That does not mean this site is affected — sites on current versions are already patched, and this scan can't see installed versions. It does mean these plugins are actively probed by attackers, so keep them updated promptly (or set to auto-update). Source: Wordfence Intelligence.

- <sup>a</sup> **google-analytics-premium** — 1 disclosure on record; latest fix in v8.15
- <sup>a</sup> **wpforms** — 3 disclosures on record; latest fix in v1.8.5.4
- <sup>a</sup> **perfmatters** — 9 disclosures on record; latest fix in v2.6.5
- <sup>a</sup> **optinmonster** — 6 disclosures on record; latest fix in v2.16.2

# Stack & security snapshot

|                        |                 |
|------------------------|-----------------|
| PLATFORM               | WEB SERVER      |
| WordPress              | cloudflare      |
| SSL CERTIFICATE        | SITEMAP         |
| Valid · 48d left       | Present         |
| EMAIL SPOOFING (DMARC) | STRUCTURED DATA |
| Protected              | Present         |
| META DESCRIPTION       | MOBILE VIEWPORT |
| Present                | Configured      |

## What this means for your business

Your site scored 83/100 on the GlossyDev index — a weighted blend of real performance, accessibility, SEO, security posture, and stack maintainability. The items above are ordered so the highest-impact fixes come first.

Most are addressable quickly, and several compound — faster load times lift both conversions and search rankings at once. We're happy to walk through the report and map the fastest path to a better score.

This analysis uses a deliberately lightweight, non-intrusive scan — it reads only what your site publicly serves to any visitor or search engine and avoids aggressive probing that could trip security tools, rate limits, or bot protection. On sites behind heavy caching, a CDN, or firewall/bot protection, some technical details (particularly platform and server detection) may be incomplete or approximate.