

🔊 LUISTER DIT VERSLAG

-10%

1,0x

+10%

+25%

1,0x

↓ Download naar telefoon

Read-only audit van **haarvisie.nl** (22-06-2026). Alles zelf geverifieerd met curl/openssl. De site is **niet aangeraakt** — puur onderzocht. Hieronder een developer-klare lijst, gesorteerd op urgentie.

📧 Stuur naar Gerrie

Stack: WordPress 7.0 + Avada-thema (+ child) + plugins (Fusion Builder/Core, WP Rocket 3.21.1, GS Pinterest Portfolio Pro, Testimonial Pro, Site Kit by Google). Server: nginx.

Top 5 meest urgent

1. **Geen enkele HTTP security header** (HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy ontbreken allemaal) — HOOG
2. **xmlrpc.php pingback staat aan** (DDoS-versterking + brute-force) — HOOG
3. **PHPSESSID-cookie zonder Secure/HttpOnly** — MIDDEN/HOOG
4. **TLS 1.1 staat nog open** (verouderd protocol) — MIDDEN
5. **readme.html publiek bereikbaar** (verklapt WordPress + versie) — MIDDEN

1. Beveiliging

- **HOOG — Security headers ontbreken volledig.** `curl -I` toont geen HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy of Permissions-Policy. Kwetsbaarder voor clickjacking, MIME-sniffing, SSL-stripping. *Advies:* toevoegen in nginx (minimaal HSTS, X-Frame-Options SAMEORIGIN, X-Content-Type-Options nosniff, Referrer-Policy strict-origin-when-cross-origin).

- **HOOG** — **xmlrpc.php met pingback actief.** `POST /xmlrpc.php system.listMethods` geeft `pingback.ping` ; een echte pingback werd geaccepteerd (geen blokkade). Misbruikroute voor brute-force + DDoS. *Advies:* `xmlrpc.php` blokkeren in nginx (tenzij Jetpack/app het echt nodig heeft).
 - **MIDDEN/HOOG** — **PHPSESSID-cookie zonder Secure/HttpOnly/SameSite.** Cookie leesbaar voor JavaScript, kan over http lekken. *Advies:* `session.cookie_secure` + `cookie_httponly` + `SameSite=Lax` ; én uitzoeken waarom de homepage een PHP-sessie start.
 - **MIDDEN** — **TLS 1.1 nog toegestaan.** `openssl s_client -tls1_1` verbindt. Verouderd. *Advies:* in nginx alleen TLS 1.2 + 1.3.
 - **MIDDEN** — **readme.html publiek (200).** Verklapt WordPress + versie-hint. *Advies:* in nginx `deny` (regeneert bij elke update).
 - **MIDDEN** — **WordPress-versie zichtbaar.** HTML bevat `meta generator: WordPress 7.0` + plugin-versies. *Advies:* generator-meta verwijderen.
 - **LAAG** — **wp-login.php open** (geen 2FA/rate-limit zichtbaar). *Advies:* brute-force-bescherming + 2FA.
 - **GOED (geen actie):** `wp-config.php` leeg (geen lek) · `/wp-json/wp/v2/users = 401` (geen username-enumeratie) · `/?author=1 = 404` · `/.git/` en `debug.log = 404` · `/wp-content/uploads/ = 403` (geen directory listing).
-

2. Performance

- **MIDDEN** — **Zware homepage-HTML (~673 KB).** 105 script-tags, 84 img-tags, ~408 resource-verwijzingen. Trager op mobiel. *Advies:* scripts uitstellen/bundelen, ongebruikte plugins heroverwegen (2x Pinterest-portfolio + testimonial), afbeeldingen verder optimaliseren.
 - **GOED:** laadtijd 0,20 s (TTFB 0,07 s) · Brotli-compressie actief · caching 1 jaar op assets · geen mixed content.
-

3. SEO

- **MIDDEN** — **Twee H1's op de homepage** (beide Avada Fusion-titles). *Advies:* één H1, rest H2.

- **MIDDEN** — **robots.txt** is leeg (0 bytes). Geen sitemap-verwijzing. *Advies:* minimaal Sitemap: `https://www.haarvisie.nl/sitemap_index.xml` toevoegen + disallow `/wp-admin/`.
 - **LAAG** — **sitemap** bestaat (`/sitemap_index.xml` = 200) maar niet in robots. *Advies:* sitemap-URL in robots.txt.
 - **GOED:** title + meta description correct + goede lengte · canonical correct · 6 Open Graph-tags + 4x schema.org JSON-LD · indexeerbaar · geen hreflang nodig (NL-site).
-

4. Techniek / hygiëne

- **LAAG** — **Dubbele redirect-hop:** `http-nonwww` → `https-nonwww` → `https-www` (2 hops). *Advies:* nginx direct naar `https://www.haarvisie.nl/` .
- **GOED:** nginx zonder versie-lek · PHP-versie niet zichtbaar · HTTP→HTTPS redirect werkt · www-canonicalisatie werkt · echte 404 (geen soft-200) · SSL-cert geldig (Let's Encrypt, 5 jun → 3 sep 2026, auto-renew).

Vastgesteld via `curl -I` / `curl -s` op `haarvisie.nl + www`, `openssl s_client` (TLS/cert), `POST` naar `/xmlrpc.php` (pingback), en `grep` op de homepage-HTML. Niets gewijzigd.