 LUISTER DIT VERSLAG

-10% 1,0x +10% +25% 1,0x

⬇ Download naar telefoon

Tweede, **diepere** beveiligingscheck van haarvisie.nl — uitgevoerd volgens de professionele methode (OWASP Web Security Testing Guide + de checks die security-auditors standaard doen). Alles is **read-only**: er is niets aan de site gewijzigd of aangevallen, alleen bekeken wat van buitenaf zichtbaar is. Deze keer met meer diepgang dan de eerste check — en met nieuwe bevindingen.

Samenvatting

De **basisbeveiliging is op orde** (moderne TLS, geen gebroken instellingen, Wordfence schermt veel af). Maar er zijn **2 belangrijke gaten** die in de eerste check niet naar boven kwamen, plus een paar kleinere info-lekken. Het grootste nieuwe punt: **iemand kan nu nep-e-mails sturen namens @haarvisie.nl** (spoofing) zonder dat ze tegengehouden worden.

Belangrijkste risico's (eerst aanpakken)

1. E-mailspoofing is niet geblokkeerd (DMARC staat op "p=none") — NIEUW

- **Bevinding:** er is een DMARC-record, maar het staat op `p=none`. Dat betekent: alleen meekijken, **niets tegenhouden**.
- **Waarom gevaarlijk:** iemand kan e-mails sturen die er uitzien alsof ze van **@haarvisie.nl** komen (naar klanten, naar je team, naar jou) — phishing/oplichting in jouw naam. Met `p=none` worden die niet afgewezen.
- **Oplossing:** DMARC eerst op `p=quarantine` zetten (verdachte mail naar spam), daarna op `p=reject` (helemaal blokkeren). Tegelijk SPF strakker zetten (zie punt 6).

2. xmlrpc.php staat open (HTTP 200)

- **Bevinding:** bevestigd, staat nog steeds open.

- **Waarom gevaarlijk:** bekend doelwit voor brute-force-inlogpogingen en het versterken van aanvallen (DDoS).
- **Oplossing:** uitschakelen. *(Op zustersite haartips.nl is dit al dicht.)*

🟡 Belangrijke verbeterpunten

3. Geen beveiligings-headers

De site stuurt geen HSTS, X-Frame-Options, Content-Security-Policy, X-Content-Type-Options, Referrer-Policy of Permissions-Policy mee. Beschermt o.a. tegen clickjacking en afdwingen van https. → Toevoegen in de nginx-config.

4. `/readme.html` staat open (HTTP 200) — NIEUW

Dit standaard WordPress-bestand is publiek bereikbaar en verklapt systeeminfo. → Verwijderen of blokkeren.

5. Plugin-versies lekken in de paginacode — NIEUW

Twee plugins tonen hun exacte versie: **gs-pinterest-portfolio (v1.9.1)** en **testimonial-pro (v3.2.3)**. Daarmee kan een aanvaller gericht zoeken of net díe versie een bekend lek heeft. *(De Avada/Fusion-bestanden gebruiken gelukkig cache-tijdstempels i.p.v. echte versies — dat is goed.)* → Plugins up-to-date houden + versie-nummers verbergen.

🟢 Kleinere punten

6. **SPF staat op `~all` (softfail)** i.p.v. `-all` (hardfail) — samen met de DMARC-fix strakker zetten. — NIEUW
7. **WordPress-versie zichtbaar** in de paginacode ("WordPress 7.0"). → verbergen.
8. **Geen security.txt** (`/.well-known/security.txt`) — een bestandje met een security-contact is best-practice zodat onderzoekers lekken netjes kunnen melden. → toevoegen. — NIEUW
9. **Content sinds ~5 april niet ververst** — telt voor Google/AI-vindbaarheid (geen beveiliging, wel belangrijk).

✳ Wat juist GOED beveiligd is (ook gecontroleerd)

Een eerlijke audit toont ook wat sterk is:
- **Geen gebruikers-enumeratie**: de WordPress-API (`/wp-json/wp/v2/users`) is afgeschermd (401) en `?author=1` is geblokkeerd. Aanvallers kunnen geen inlognamen oogsten.
- **Geen blootgestelde gevoelige bestanden**: `.git` , `.env` , `wp-config` -backups en `debug.log` zijn allemaal niet bereikbaar.
- **Geen directory listing** (uploads-map geeft 403).
- **Alleen moderne TLS**: de oude, onveilige protocollen TLS 1.0 en 1.1 staan uit.
- **DNSSEC staat aan** (bescherming tegen DNS-vervalsing).
- **http wordt afgedwongen naar https** (301).
- **SSL geldig** en automatisch vernieuwd.

✳ Prioriteitslijst voor de beheerder

1. **DMARC** naar `p=quarantine` → later `p=reject` (stopt e-mailspoofing).
2. **xmlrpc.php** uitschakelen.
3. **Beveiligings-headers** toevoegen (nginx).
4. **`/readme.html`** verwijderen/blokkeren.
5. **Plugins updaten** + versie-nummers verbergen.
6. **SPF** op `-all` , **WP-versie** verbergen, **security.txt** toevoegen.

Expert-audit 23-06-2026 volgens OWASP-methodiek, volledig read-only (haarvisie.nl is niet gewijzigd of aangevallen — alleen van buitenaf bekeken). Vergeleken met de eerste check zijn dit de nieuwe bevindingen: e-mailspoofing (DMARC), readme.html, plugin-versie-lekken, SPF-softfail en het ontbreken van security.txt. De basis blijkt sterker dan gedacht (geen user-enumeratie, geen blootgestelde bestanden, moderne TLS, DNSSEC).