 LUISTER DIT VERSLAG

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

⬇ Download naar telefoon

Objectieve, technische momentopname van haarvisie.nl op 23 juni 2026. Dit is een **read-only controle** (er is niets gewijzigd aan de site) om een eerlijk beeld te krijgen van hoe de site onderhouden en beveiligd is. Bedoeld als constructieve input — met per punt de uitleg én de oplossing.

Samenvatting

De **basis staat goed**: de site is veilig bereikbaar, up-to-date en beschermd met een beveiligingsplugin. Maar de **afwerking en het proactieve onderhoud blijven achter**: een paar standaard beveiligings-instellingen ontbreken, en de content wordt al ~2,5 maand niet ververst. Kortom: het onderhoud is **reactief, niet proactief**.

Eindoordeel: voldoende, maar niet top.

✳ Wat goed geregeld is

- **SSL-certificaat** is geldig en wordt automatisch vernieuwd (loopt door tot 3 september 2026). Bezoekers zitten veilig op `https`.
- **WordPress is up-to-date** (versie 7.0, de nieuwste). Goede basishygiëne.
- **Beveiligingsplugin (Wordfence) actief** — gebruikersnamen worden netjes afgeschermd (geen makkelijke doelwitten voor inlogpogingen).
- **Site is online, snel en stabiel.**

⚠ Wat beter kan (met uitleg + oplossing)

1. xmlrpc.php staat open (belangrijkste punt)

- **Bevinding:** `xmlrpc.php` reageert met HTTP 200 — dit onderdeel staat open.
- **Waarom een risico:** xmlrpc is een bekend doelwit voor misbruik — aanvallers gebruiken het voor brute-force-inlogpogingen en om aanvallen te versterken (DDoS-amplificatie). Vrijwel geen enkele moderne site heeft het nog nodig.
- **Oplossing:** xmlrpc uitschakelen (via de webserver of een plugin). *(Ter vergelijking: op de zustersite haartips.nl is dit al dichtgezet.)*

2. Beveiligings-headers ontbreken

- **Bevinding:** de site stuurt geen beveiligings-headers mee (geen HSTS, X-Frame-Options, X-Content-Type-Options, Content-Security-Policy, Referrer-Policy of Permissions-Policy).
- **Waarom een risico:** deze headers beschermen onder andere tegen "clickjacking" (je site in een nep-frame), tegen het verkeerd interpreteren van bestanden, en dwingen altijd-https af. Dit is standaard basis-hygiëne voor een professionele site.
- **Oplossing:** deze headers toevoegen in de nginx-configuratie (eenmalig werk, daarna klaar).

3. WordPress-versie zichtbaar in de code

- **Bevinding:** in de paginacode staat letterlijk `WordPress 7.0` .
- **Waarom een risico:** dat verklapt precies welke versie je draait. Zodra er ooit een lek in een versie bekend wordt, weten aanvallers meteen of jouw site kwetsbaar is. Klein, maar onnodig info-lek.
- **Oplossing:** de versie-vermelding (de "generator"-tag) verbergen.

4. Content al ~2,5 maand niet ververst

- **Bevinding:** de laatste inhoudelijke update was rond 5 april 2026.
- **Waarom belangrijk:** Google én AI-zoekmachines (ChatGPT, Gemini) geven verse content voorrang. Stilstaande content zakt langzaam weg in de zoekresultaten.
- **Oplossing:** regelmatig (bijv. maandelijks) iets verversen — een blog, een tekst, een actie.

Conclusie

Iemand houdt de boel **bij** — SSL, updates en de beveiligingsplugin zijn op orde, en dat is belangrijk. Maar een **echt sterke beheerder** had de open xmlrpc, de ontbrekende

beveiligings-headers en de zichtbare versie allang dichtgetimmerd, en zou de content actiever vers houden. Dit zijn standaard punten die bij proactief onderhoud horen.

Geen van deze punten is een acuut noodgeval, maar samen laten ze zien dat het onderhoud nu vooral **reactief** is. Met een paar uur werk staat de afwerking netjes.

Aanbevolen acties (op prioriteit)

1. **xmlrpc.php uitschakelen** (belangrijkste).
2. **Beveiligings-headers toevoegen** in de webserver-config.
3. **WordPress-versie verbergen** in de code.
4. **Content-ritme afspreken** (bijv. maandelijks verversen).

Momentopname 23-06-2026, volledig read-only opgehaald (er is niets aan haarvisie.nl gewijzigd). Alle bevindingen zijn van buitenaf zichtbaar en op de meetdatum geverifieerd. Bedoeld als objectieve, constructieve input.