

IQ ICT | Wordpress Scan

Geavanceerde WP Scan Analyse

Klantnaam : iqwpscan.nl

Dienst: Geavanceerde WP Scan Analyse

Uitgevoerd met: Linux

Type: Analyse (analyse + advies)

Versie: 1.0

Datum: 1 oktober 2025

Klant: iqwpscan.nl

Samenvatting

De WordPress-installatie op <https://iqwpscan.nl/> draait op de nieuwste versie (6.8.3). Toch zijn er een aantal aandachtspunten die de veiligheid beïnvloeden. Hieronder volgt een overzicht van kwetsbaarheden en configuratieproblemen, inclusief aanbevelingen.

Scanresultaten

#	Bevinding	Component	Risico	Beschrijving	Aanbeveling
1	Plugin "Akismet" bevat kwetsbaarheid	Plugin	Hoog	Kwetsbaar voor Unauthenticated Stored XSS tot versie 3.1.4	Zorg dat plugin versie $\geq 3.1.5$ wordt gebruikt of schakel uit
2	Plugin "Elementor" verouderd	Plugin	Gemiddeld	Versie 3.32.1 actief, laatste versie is 3.32.3	Update naar laatste versie via dashboard
3	Plugin "WP Statistics" verouderd	Plugin	Hoog	Kwetsbaar voor Stored XSS (CVE-2025-9816) < v14.15.5	Update naar minimaal versie 14.15.5
4	Plugin "WPForms Lite" verouderd	Plugin	Gemiddeld	Versie 1.9.7.3 actief, laatste is 1.9.8.1	Update via pluginscherm
5	readme.html aanwezig	Core bestand	Laag	Bevat WordPress versie-informatie, nuttig voor aanvallers	Verwijder of beperk toegang via .htaccess
6	robots.txt onthult admin-paden	Configuratie	Laag	/wp-admin/ zichtbaar	Beperk toegang via IP of 2FA
7	wp-cron.php publiek benaderbaar	Core functionaliteit	Laag	Kan bij veel verkeer misbruikt worden voor DDoS	Overweeg om WP Cron extern te beheren
8	MU-plugins directory publiek zichtbaar	Plugins	Gemiddeld	Must Use Plugins zijn detecteerbaar	Verberg of beveilig toegang via serverinstellingen
9	Gebruiker "adminuser" publiek zichtbaar	Gebruiker	Laag	Gebruikersnamen beschikbaar via JSON API	Overweeg REST API-beperking met plugin
10	Meerdere thema's aanwezig	Thema's	Laag	Overtollige thema's kunnen risico vormen als ze niet up-to-date zijn	Verwijder ongebruikte thema's

Aanbevelingen

1. Pluginbeheer

- Werk kwetsbare plugins **Akismet**, **WP Statistics** en **WPForms Lite** bij
- Controleer regelmatig plugins op updates en CVE's

2. Core-beveiliging

- Verwijder readme.html uit de rootmap
- Beperk toegang tot /wp-admin/ waar mogelijk
- Beheer wp-cron.php via externe cron als alternatief

3. Gebruikers & API

- Overweeg om gebruikersnamen af te schermen via plugins zoals "Disable REST API"

4. Thema's opschonen

- Verwijder inactieve thema's die niet gebruikt worden
- Controleer of actieve thema's actueel zijn

5. Server- & bestandsbeveiliging

- Blokkeer toegang tot MU-plugins en gevoelige paden via .htaccess
- Voeg beveiligingsheaders toe waar mogelijk:
- Header set X-Content-Type-Options "nosniff"
- Header set X-Frame-Options "SAMEORIGIN"
- Header set Content-Security-Policy "default-src 'self';"