

🔊 LUISTER DIT VERSLAG

-10%

1,0x

+10%

+25%

1,0x

↓ Download naar telefoon

Soort: vergadering · **Duur:** onbekend · **Deelnemers:** [Speaker 1] [Speaker 2]

Let op — sprekers niet bevestigd. Plaud nummert sprekers (Speaker 1, 2, ...) maar koppelt geen namen. Ga niet uit van wie wat zei; "ik/wij" hoeft niet dezelfde persoon te zijn.

Notulen

AI-agenten integreren met WordPress

De discussie richt zich op het mogelijk maken voor AI-agenten om op maat gemaakte tools binnen een WordPress-omgeving zelfstandig te gebruiken.

De huidige methode, een "browser bridge", is onhandig en breekbaar, waardoor agenten de weg kwijtraken.

Het doel is een robuuste, veilige en voorspelbare oplossing te vinden.

De rol van het Model Context Protocol (MCP)

MCP wordt geïntroduceerd als kernoplossing: een universele standaard vergelijkbaar met een USB-poort voor AI.

Het stelt AI-agenten in staat direct met WordPress te communiceren in een gedeelde taal, in plaats van via een visuele interface.

Automattic (het bedrijf achter WordPress.com) heeft sinds maart 2026 volledige "write"-mogelijkheden via MCP geïntroduceerd, met menselijke goedkeuring.

Dit is ook beschikbaar voor zelfgehoste WordPress-sites via plugins.

Technische implementatie in WordPress

Stap 1: MCP-server installeren:

Gebruik de officiële "WordPress MCP Adapter" plugin van Automattic.

Deze plugin werkt samen met de "Abilities API", beschikbaar sinds WordPress 6.9.

Stap 2: Rechten instellen en verbinden:

De "Abilities API" definieert specifieke toegestane acties voor een agent (bijv. conceptpost aanmaken, afbeelding uploaden).

Beveilig de verbinding door een "application-password" te genereren in WordPress en deze in de configuratie van de AI-agent te plaatsen.

Agentvriendelijke interfaces ontwerpen

Een veelgemaakte fout is het gebruik van één groot tekstveld voor een prompt.

Oplossing: Gestructureerde invoervelden (Structured Prompt Fields):

Breek de invoer op in logische, aparte velden (bijv. onderwerp, stijl, kleurenpalet).

Dit maakt de interactie voorspelbaar en vermindert dubbelzinnigheid voor de agent.

Knoppen en UI-elementen:

Geef cruciale knoppen een duidelijke en vaste HTML-ID (bijv.

ID="GenerateImageButton"

).

Consistentie in de UI is essentieel om te voorkomen dat agenten de weg kwijtraken.

Veiligheid en controle

Regel 1: Nooit direct publiceren.

De standaardactie voor een AI-agent moet altijd "opslaan als concept" zijn. Publicatie vereist een menselijke controle.

Tools voor extra veiligheid:

Tools zoals "WP Navigator" bieden een "preview-diff" (voor- en navergelijking) voordat een wijziging wordt doorgevoerd.

Deze systemen bevatten vaak een "kill switch" om een agent direct te stoppen en een "rollback"-functie.

Foutafhandeling:

Tools moeten gestructureerde foutmeldingen teruggeven die een agent kan interpreteren, in plaats van alleen een visuele foutmelding.

Concreet actieplan

Het gesprek wordt samengevat in een vierstappenplan:

Omarm de standaard:

Implementeer het Model Context Protocol (MCP).

Installeer de MCP-server:

Gebruik de "WordPress MCP Adapter" plugin.

Herontwerp de interface:

Gebruik gestructureerde velden en consistente ID's.

Veiligheid eerst:

Laat agenten opslaan als concept en gebruik tools voor extra controle.

Volgende stappen

De interface van de afbeeldingengenerator ombouwen naar gestructureerde velden.

De "WordPress MCP Adapter" plugin installeren.

Tools zoals WP Navigator onderzoeken voor extra controle en veiligheid.

Plan opstellen voor gestructureerde foutafhandeling (specifieke error-codes en -formatten).

Vergelijking uitvoeren van MCP-plugins ("Vibe AI", "Easy MCP AI") versus de aanbevolen "WordPress MCP Adapter" (voor- en nadelen, compatibiliteit, beveiliging).

AI-suggesties

AI-suggesties

AI heeft de volgende problemen geïdentificeerd die niet zijn afgesloten in de vergadering of waarvoor duidelijke actiepunten ontbreken; gelieve hier aandacht aan te besteden:

Er is geen specifiek actiepunt vastgelegd voor het implementeren van gestructureerde foutafhandeling, wat cruciaal is om te voorkomen dat AI-agenten vastlopen bij fouten.

De discussie noemt verschillende MCP-plugins ("Vibe AI", "Easy MCP AI"), maar er is geen plan om de voor- en nadelen hiervan te vergelijken met de aanbevolen "WordPress MCP Adapter".