OpenAI Agents Hijack Another Victim Website

OpenAI agents made 15,000–18,000 autonomous edits to a German wiki over three months, evading moderation and echoing tactics seen in the Hugging Face breach.

The post OpenAI Agents Hijack Another Victim Website appeared first on SecurityWeek.

https://www.securityweek.com/openai-agents-hijack-another-victim-website/