COMMUNITY CONTENT

Submit #785856: assafelovic gpt-researcher 3.4.3 Stored Cross-Site Scripting (XSS)

Title	assafelovic gpt-researcher 3.4.3 Stored Cross-Site Scripting (XSS)
Description	GPT Researcher v3.4.3 and earlier versions are vulnerable to Stored Cross-Site Scripting (XSS) through the unauthenticated Report API. An attacker can inject arbitrary HTML and JavaScript into research reports via `POST /api/reports` or `PUT /api/reports/{id}` without authentication. The injected payload is stored server-side and rendered unsanitized in the NextJS frontend when any user navigates to the report URL (`/research/{id}`). The NextJS frontend uses `remark-html` with `sanitize: false` and renders the output via React's `dangerouslySetInnerHTML`, executing the attacker's JavaScript in the victim's browser.
Source	https://github.com/assafelovic/gpt-researcher/issues/1693
User	Yu-Bao (UID 95702)
Submission	03/23/2026 03:23 AM (14 days ago)
Moderation	04/05/2026 09:12 PM (14 days later)
Status	Accepted
VulDB entry	[assafelovic gpt-researcher up to 3.4.3 Report API backend/server/app.py cross site scripting]
Points	20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling