COMMUNITY CONTENT

Home › Submit › 781810

Submit #781810: 1Panel-dev MaxKB <= v2.2.1 Stored XSS

Title	1Panel-dev MaxKB <= v2.2.1 Stored XSS
Description	Maxkb is vulnerable to Stored Cross-Site Scripting (XSS) due to a lack of HTML escaping when processing application names and icons. An authenticated user can create an application with a malicious payload in the application name. When any user visits the public chat interface (/ui/chat/{access_token}), StaticHeadersMiddleware performs unescaped string replacement to inject the application data directly into the HTML response. This allows the attacker to break out of the <title> tag and execute arbitrary JavaScript in the victim's browser context.
Source	⚠ https://github.com/AnalogyC0de/public_exp/issues/23
User	Ana10gy (UID 93358)
Submission	03/17/2026 05:30 PM (27 days ago)
Moderation	04/11/2026 09:35 AM (25 days later)
Status	Accepted
VulDB entry	356965 [1Panel-dev MaxKB up to 2.2.1 Public Chat Interface static_headers_middleware.py StaticHeadersMiddleware Name 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