COMMUNITY CONTENT

Home › Submit › 785563

Submit #785563: givanz VvvebJs 2.0.5 Stored XSS

Title	givanz VvvebJs 2.0.5 Stored XSS
Description	1. Unauthenticated Access & Stored XSS: - A critical vulnerability exists in the upload.php endpoint of VvvebJs. The endpoint completely lacks authentication and access control mechanisms by default. - An unauthenticated, remote attacker can directly send a POST request to upload files. Furthermore, the endpoint fails to sanitize the contents of uploaded SVG (Scalable Vector Graphics) files. 2. Exploiting the Vulnerability: - Because SVG is an XML-based format that supports embedded JavaScript via attributes like onload, an attacker can upload a maliciously crafted .svg file containing arbitrary JavaScript code. - Once the file is uploaded, it is stored in the /media/ directory. When any user (including administrators) accesses the direct URL of the uploaded SVG file, their browser parses the file and executes the embedded JavaScript payload within the context of the application's domain.
Source	https://tcn60zf28jhk.feishu.cn/wiki/Cr4KwlMPiMi65fFkl9Vyc3oX2h0f?from=from_copylink
User	EthXO_ (UID 96627)
Submission	03/22/2026 12:20 PM (15 days ago)
Moderation	04/05/2026 05:32 PM (14 days later)
Status	Published
VulDB entry	[givanz Vvvebjs up to 2.0.5 File Upload Endpoint upload.php uploadAllowExtensions 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