Unauthenticated Stored XSS = 2.0.5

Modified March 22

BUG_Author: EthX0_

Affected Version: VvvebJs = 2.0.5

Vendor: givanz GitHub Repository

Software: VvvebJs

Vulnerability Files:

- `upload.php`

Description:

1. **Unauthenticated Access & Stored XSS:**
   - A critical vulnerability exists in the `upload.php` endp authentication and access control mechanisms by defa
   - An unauthenticated, remote attacker can directly send endpoint fails to sanitize the contents of uploaded SVG
2. **Exploiting the Vulnerability:**
   - Because SVG is an XML-based format that supports e attacker can upload a maliciously crafted `.svg` file c
   - Once the file is uploaded, it is stored in the `/media/` accesses the direct URL of the uploaded SVG file, the JavaScript payload within the context of the applicatio

Proof of Concept:

Step 1: Uploading the Malicious SVG (Unauthenticated) A request to upload the malicious SVG file (`testtest.svg`)