

FuguHub 8.1 Reflected SVG XSS Vulnerability Report

Discovered by: Foo Han Tek

Date: 12 November 2025

Impact: Reflected Cross-Site Scripting (XSS)

Severity: High

1. Introduction

FuguHub is a cloud-based media server developed by Real Time Logic / Sesamt Data AB. During testing of a default installation, a reflected cross-site scripting (XSS) vulnerability was identified in the handling of SVG files served through FuguHub's built-in file manager.

Malicious JavaScript embedded inside an SVG file is executed automatically when the file is opened via the `/fs/` interface. This allows remote attackers to execute arbitrary JavaScript in the victim's browser.

2. Test Environment

- Operating System: Debian Linux (fresh installation)
- FuguHub Version: Latest download as of **2025-11-12**

URL tested:

`http://127.0.0.1/fs/`

FuguHub does not display an explicit version number in the UI. Testing was performed on a clean installation directly from the official download page.

Proof of Concept

First, download and run the latest version of FuguHub:

```
wget FuguHub.com/install/FuguHub.linux.install
chmod +x FuguHub.linux.install
sudo ./FuguHub.linux.install
```

- i. Go to Web-File-Server section and go to Web File Manager:

Web File Server
(Web-File-Manager and WebDAV links)

You are not accessing your server from a remote computer! [What does this mean?](#)

The Web File Manager and WebDAV provide services similar to file sharing software, thus enabling users to easily upload and download files.

1. Access the WebDAV server by using a [WebDAV client](#). A WebDAV client can map/mount the FuguHub WebDAV server as an external drive.
2. Access the Web File Manager using a web browser such as Safari, Chrome, Internet Explorer, Firefox, etc.

Click one of the links shown in the table below to access the Web File Manager (2):

File Server Links	Access Rights
/fs/	read - write

Connect WebDAV (1):
You appear to be using Linux. See our [Linux WebDAV Tutorial](#) for how to connect your Linux as a WebDAV client.

- ii. In Web File Manager, upload xss.svg:

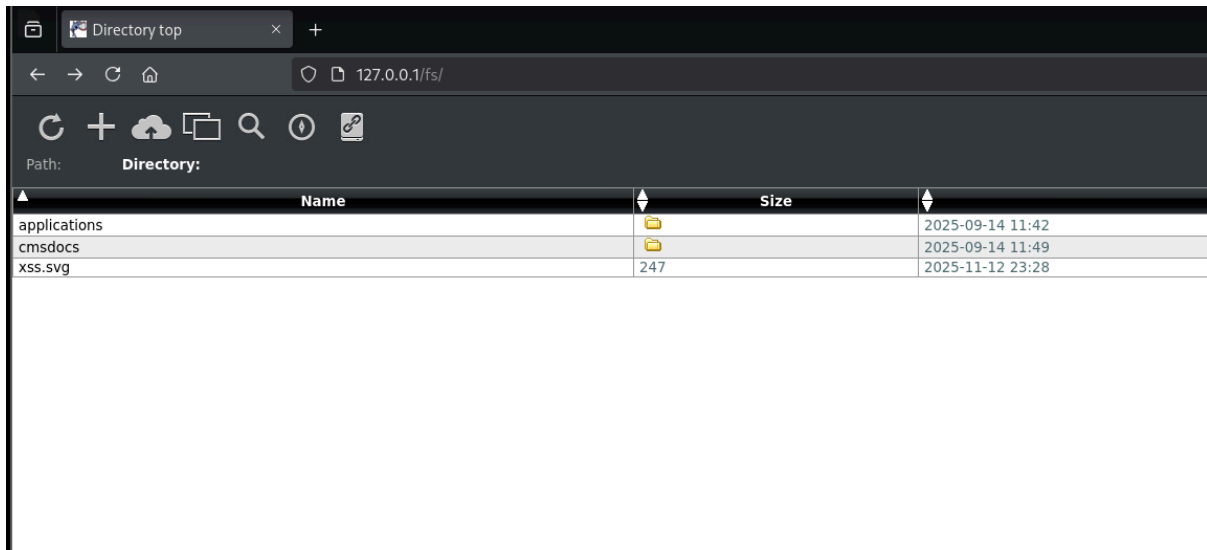
Directory top

Path: Directory:
File:

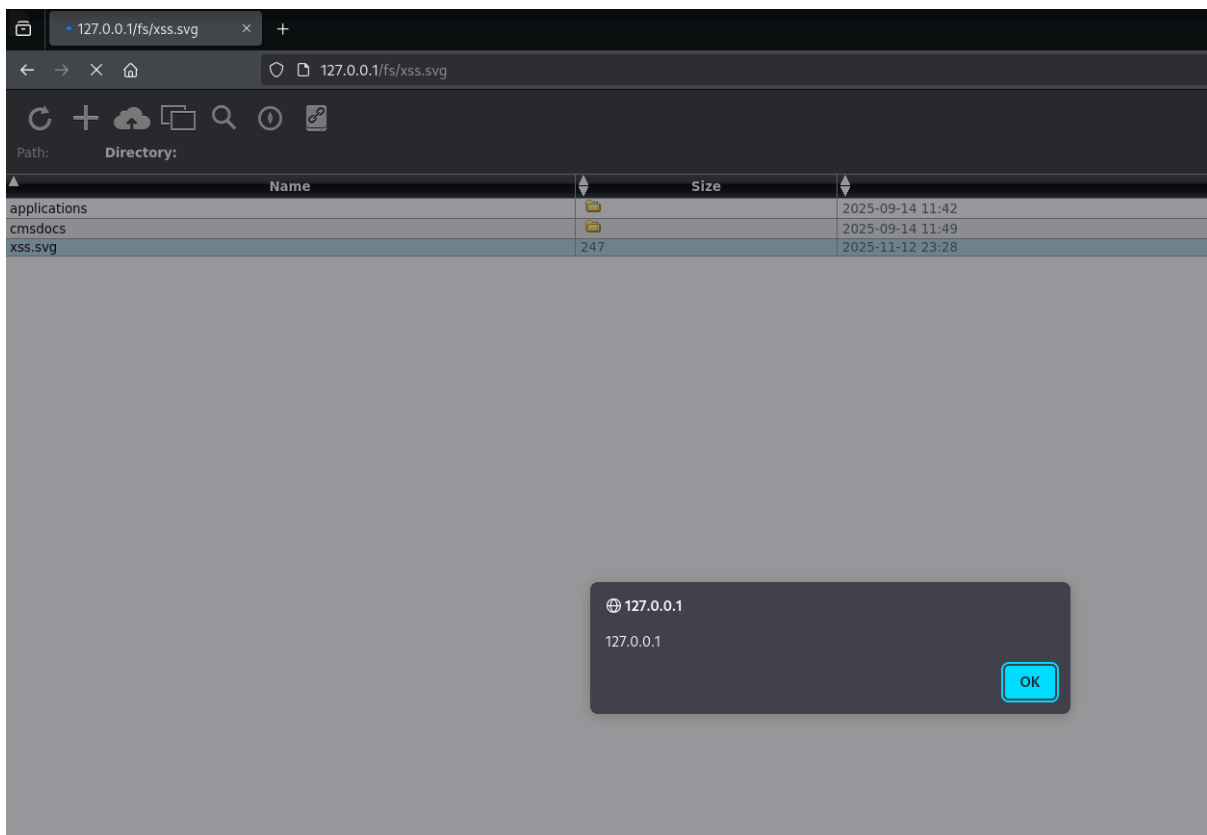
Note: Drag and drop upload is supported by this browser! Drop your file(s) into the box.

Name	Size	Local Date
applications		2025-09-14 11:42
cmsdocs		2025-09-14 11:49
xss.svg	247	2025-11-12 23:28

iii. Successfully uploaded xss.svg



iv. Upon clicking xss.svg, it triggers XSS and the alert is showing the domain "127.0.0.1" via alert(document.domain)



Below is the xss.svg code I used in the PoC:

```
<svg xmlns="http://www.w3.org/2000/svg" width="400" height="400" viewBox="0 0 124 124"
fill="none">
<rect width="124" height="124" rx="24" fill="#000000"/>
  <script type="text/javascript">
    alert(document.domain);
  </script>
</svg>
```

3. Root Cause

FuguHub serves SVG files as raw XML without sanitization. Browsers treat SVG as active content and execute `<script>` blocks embedded inside the SVG. Because FuguHub performs no filtering or rewriting of SVG content, the browser executes the embedded JavaScript, resulting in reflected XSS.

4. Impact

A remote attacker who can upload or place an SVG file on the server can cause arbitrary JavaScript to be executed in the victim's browser when viewing the file in the `/fs/` file manager. This may lead to UI manipulation, phishing, session token access (if cookies are not HttpOnly), or forced actions in the application.

5. Mitigation Recommendations

- Strip `<script>` tags from SVG files before serving
- Sanitize SVG content server-side
- Block inline scripts via Content Security Policy (CSP)
- Restrict SVG upload functionality if not needed
- Convert SVGs to raster (PNG) before serving

6. CVE Status

A CVE ID has been requested from MITRE.

Status: **Pending assignment**

7. Credits

Discovered by **Foo Han Tek**