Reflected XSS through crafted filename in file upload functionality

Low **Frooodle** published **GHSA-q5j3-4m5w-wp75** 6 hours ago

Package

Stirling-PDF (Stirling-PDF)

Affected versions	Patched versions
1.3.2	2.0.0

Description

Summary

File upload endpoints in the application accept files with user-controlled filenames and reflect these filenames in the web interface without proper sanitization or escaping, enabling XSS attacks. This issue is not limited to PDF files and can be triggered with any file type.

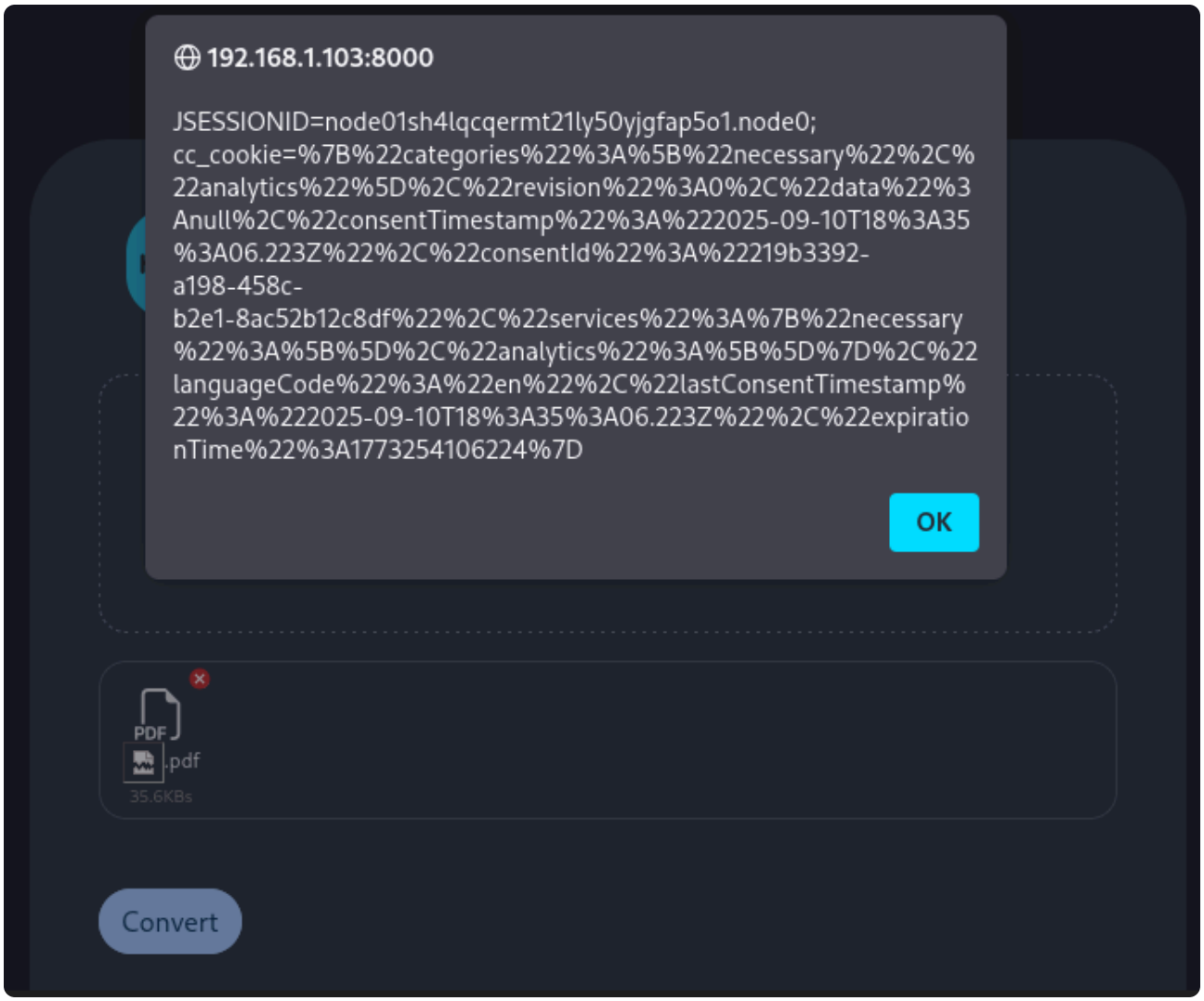
Details

The vulnerability arises because the application injects the uploaded file's name directly into HTML content using unsafe methods such as innerHTML without encoding special characters. An attacker can upload a file with a filename containing HTML or JavaScript code, like:
`<img src=x onerror=alert(document.cookie)>.pdf`
immediately causes the script to run on the upload confirmation section of the same page. The execution happens within the same browser session and page context where the upload took place.
This vulnerability is a reflected XSS, limited to the uploading user and session.
This issue is independent of the file type and affects all files uploaded through this interface.

PoC

Complete instructions, including specific configuration details, to reproduce the vulnerability.
Proof of Concept
Rename or create a file with a malicious filename, e.g. `<img src=x onerror=alert(document.cookie)>.pdf`.

Upload the file:



on any of the following upload pages:

http://ip/scale-pages
http://ip/crop
http://ip/extract-page
http://ip/merge-pdfs
http://ip/multi-page-layout
http://ip/pdf-organizer
http://ip/multi-tool
http://ip/pdf-to-single-page
http://ip/remove-pages
http://ip/rotate-pdf
http://ip/split-pdfs
http://ip/file-to-pdf
http://ip/eml-to-pdf
http://ip/html-to-pdf
http://ip/img-to-pdf
http://ip/markdown-to-pdf
http://ip/pdf-to-csv
http://ip/pdf-to-html

http://ip/pdf-to-img
http://ip/pdf-to-markdown
http://ip/pdf-to-pdfa
http://ip/pdf-to-presentation
http://ip/pdf-to-text
http://ip/pdf-to-word
http://ip/pdf-to-xml
http://ip/add-password
http://ip/stamp
http://ip/add-watermark
http://ip/change-permissions
http://ip/redact
http://ip/remove-cert-sign
http://ip/remove-password
http://ip/sanitize-pdf
http://ip/sign
http://ip/cert-sign
http://ip/validate-signature
http://ip/add-attachments
http://ip/add-image
http://ip/add-page-numbers
http://ip/replace-and-invert-color-pdf
http://ip/change-metadata
http://ip/compare
http://ip/extract-images
http://ip/flatten
http://ip/get-info-on-pdf
http://ip/ocr-pdf
http://ip/remove-annotations
http://ip/remove-blanks
http://ip/remove-image-pdf
http://ip/unlock-pdf-forms
http://ip/adjust-contrast
http://ip/auto-rename
http://ip/split-by-size-or-count
http://ip/auto-split-pdf
http://ip/compress-pdf
http://ip/extract-image-scans
http://ip/edit-table-of-contents
http://ip/overlay-pdf
http://ip/pipeline
http://ip/repair
http://ip/scanner-effect
http://ip/show-javascript
http://ip/split-pdf-by-chapters
http://ip/split-pdf-by-sections

After the upload, observe that the filename is rendered directly in the page and the embedded JavaScript code executes immediately within the user's browser context.

Impact

What kind of vulnerability is it? Who is impacted?

- This vulnerability enables reflected XSS, where only the user uploading the malicious file is affected during their active session.
- Attackers can exploit this by crafting files with malicious filenames and tricking users into uploading them, potentially leading to theft of cookies, session tokens, or other sensitive data visible to the browser.
- It can facilitate social engineering or phishing attacks by manipulating the victim’s view or injecting arbitrary scripts in their browser.
- Although it does not directly affect other users (not a stored XSS affecting multiple users), it breaks critical input validation and output encoding expectations and may lead to further impact if combined with other vulnerabilities.
- The issue affects a broad range of file upload endpoints across the application, increasing the attack surface.
- This makes the vulnerability significant enough to warrant prompt remediation to prevent exploitation and protect user security and trust.

Severity

Low 3.1 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity	None
Availability	None

Learn more about base metrics

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

CVE ID

CVE-2026-33436

Weaknesses

- CWE-20
- CWE-79
- CWE-116

Credits

Szym0n13k Reporter