CVE-2020-35240 - FluxBB 1.5.11 - 'Blog Content' Stored Cross-Site Scripting

Exploit Title: FluxBB 1.5.11 - 'Blog Content' Stored Cross-Site Scripting

Date: 03-12-2020

Exploit Author: Hemant Patidar (HemantSolo)

Vendor Homepage: https://fluxbb.org/

Software Link: https://fluxbb.org/downloads/

Version: 1.5.11

Tested on: Windows 10/Kali Linux

Stored Cross-site scripting(XSS): This vulnerability can results attacker injecting the XSS payload in "Blog Content" and each time any user will visit the blog, the XSS triggers, and the attacker can able to steal the cookie according to the crafted payload. Vulnerable Parameters: Admin Page and Blog Content.

Steps-To-Reproduce:

1. Login as FluxBB admin user.
2. Now go to the URL: https://127.0.0.1/fluxbb/post.php?action=post&fid=1
3. Now Make a new post.
4. Now enter any subject.
5. Put the payload in Content: (Decrypt using base64:
   "Pic+Ij48aW1nIHNyYz14IG9ubW91c2VvdmVyID1wcm9tcHQoZG9jdW1lbnQuZG9tYWluKT4=")
6. Now click on Save & Continue button.
7. The XSS will be triggered.