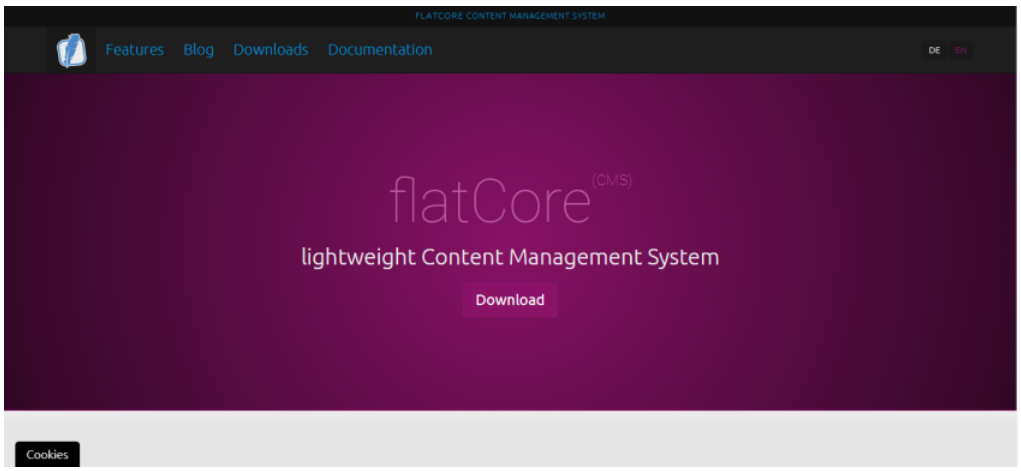
nu11secur1ty Update README.MD ... on Aug 27, 2021 History

..	
doc	last year
PWNPHPSESSID.py	last year
README.MD	last year
chromedriver.exe	last year
flatCore-CMS-2.0.7.zip	last year
pic.svg	last year

README.MD

CVE-2021-39609



Description:

Cross-Site Scripting (XSS SVG - Stored - PWNED PHPSESSID RCE) vulnerability exists in FlatCore-CMS 2.0.7 via the upload image function. When the malicious user trick the administrator of the CMS system to upload the malicious SVG file, then he can be already executed this code from everywhere on the internet, and the thing will be more worst than ever for the owner of this CMS system! ;)

@nu11secur1ty

PHPSESSID PWNED:

- Proof:
- [+] https://streamable.com/9aj8o6

XSS SVG - Stored:

- Proof:
- [+] https://streamable.com/p13hgj

Structure and tactic of the attack:

- FOR A LOT OF PEOPLE WHO DON'T REALLY `UNDERSTAND` THE PROBLEM!

1. Trick the admin of the CMS system to upload the malicious `SVG` file.
2. Execute your code remotely - RCE, example: https://targetdomain.com/flatCore-CMS-2.0.7/content/images/pic.svg
3. Get `PHPSESSID` and exploit the victim :D ;)

- Good luck :D ;)

Discusion:

- [+] href