VULNERABLE: XSS store vulnerability exists in comment add link function in Backdrop version 1.2.1 allows attackers to execute arbitrary web scripts

Date: 02/06/2022

Author: KienNT

Contact :

Github : https://github.com/Nguyen-Trung-Kien

Gmail: nguyentrungkien.31120@gmail.com

Facebook: https://www.facebook.com/anhchangmutrang.auz1/

Twitter : https://twitter.com/kienan1100

Product: Backdropcms

Vendor : Backdropcms

Description : XSS store vulnerability exists in comment add link function in Backdrop version 1.2.1 allows attackers to execute arbitrary web scripts

Impact: Attackers can masquerade as authorized users via session cookies, allowing them to perform any action allowed by the user account.

Suggestions: User input should be filter, Escaping

Payload :

- <script>alert(document.cookie)</script>

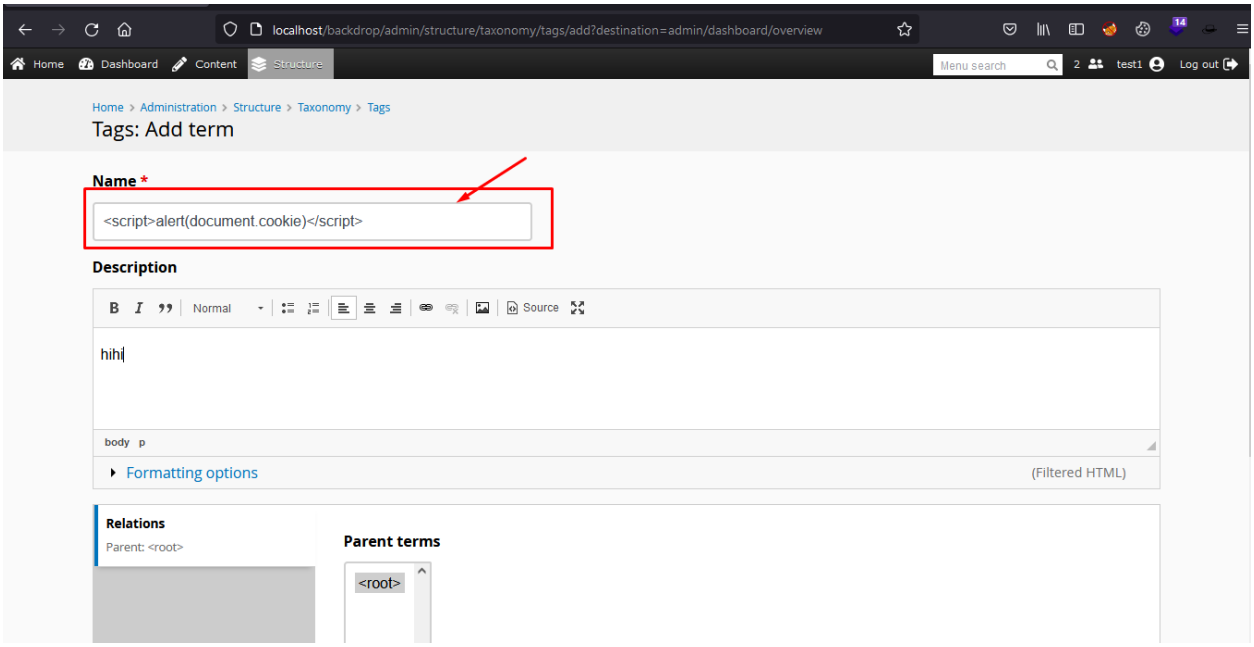
Poc:

Role: editor

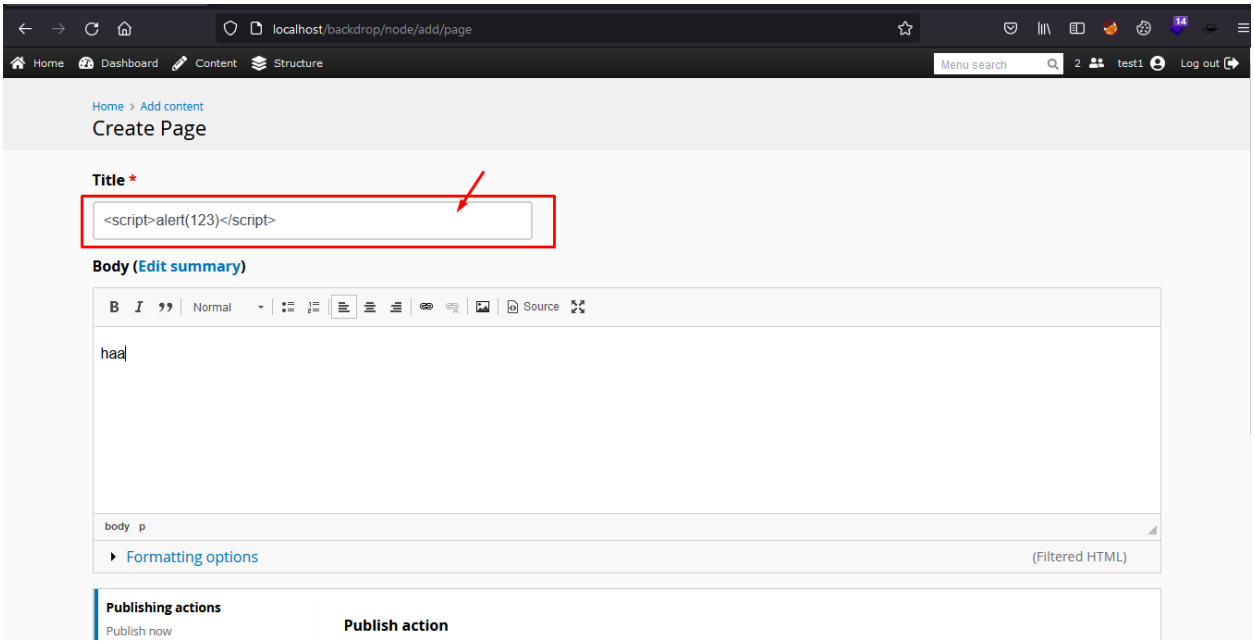
Endpoint:

- Add Tag
- Add post
- Add Page

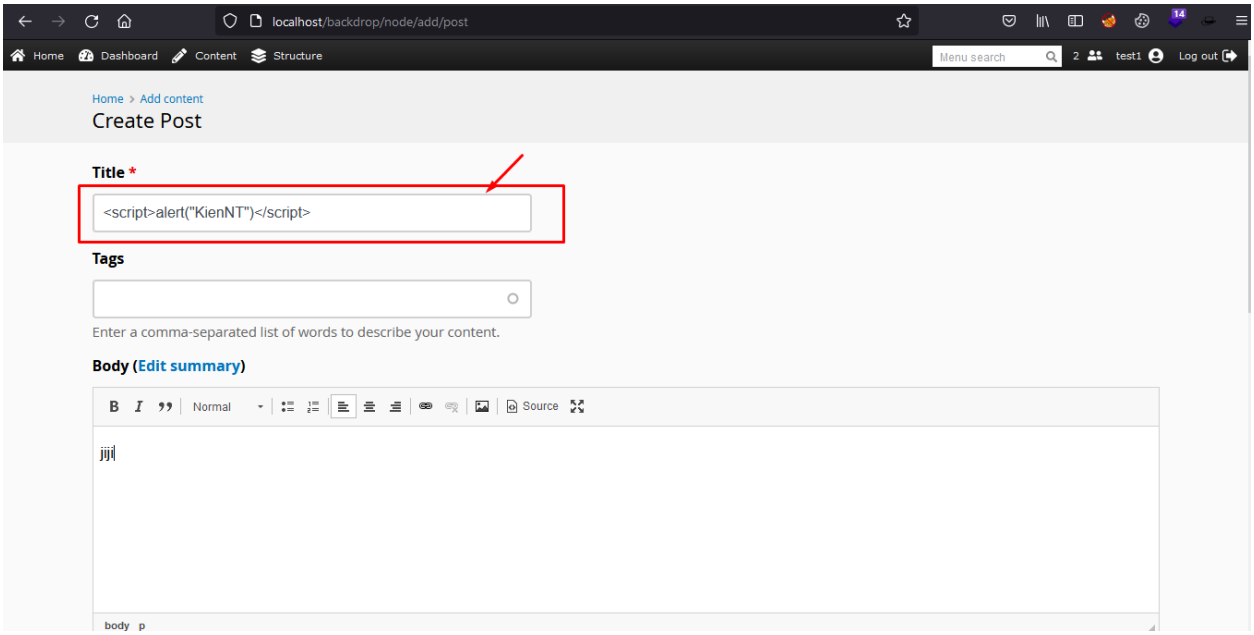
Editor can create tags,post,page and can add payload xss store



Add new tags with name endpoint

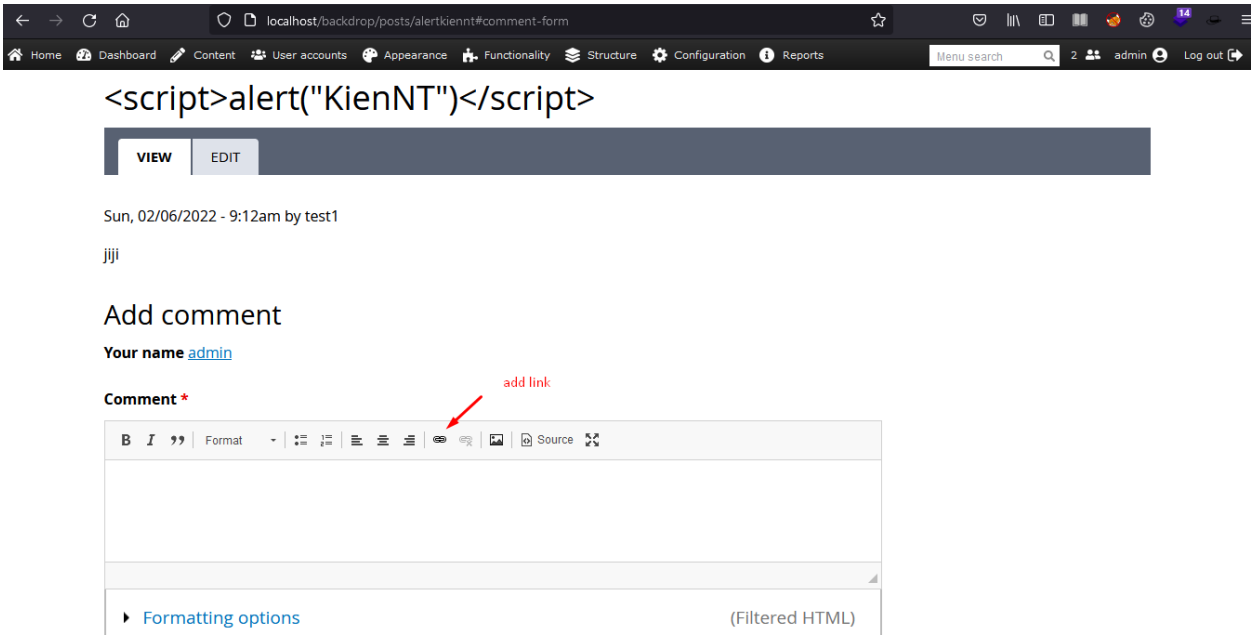


Add new page with title endpoint

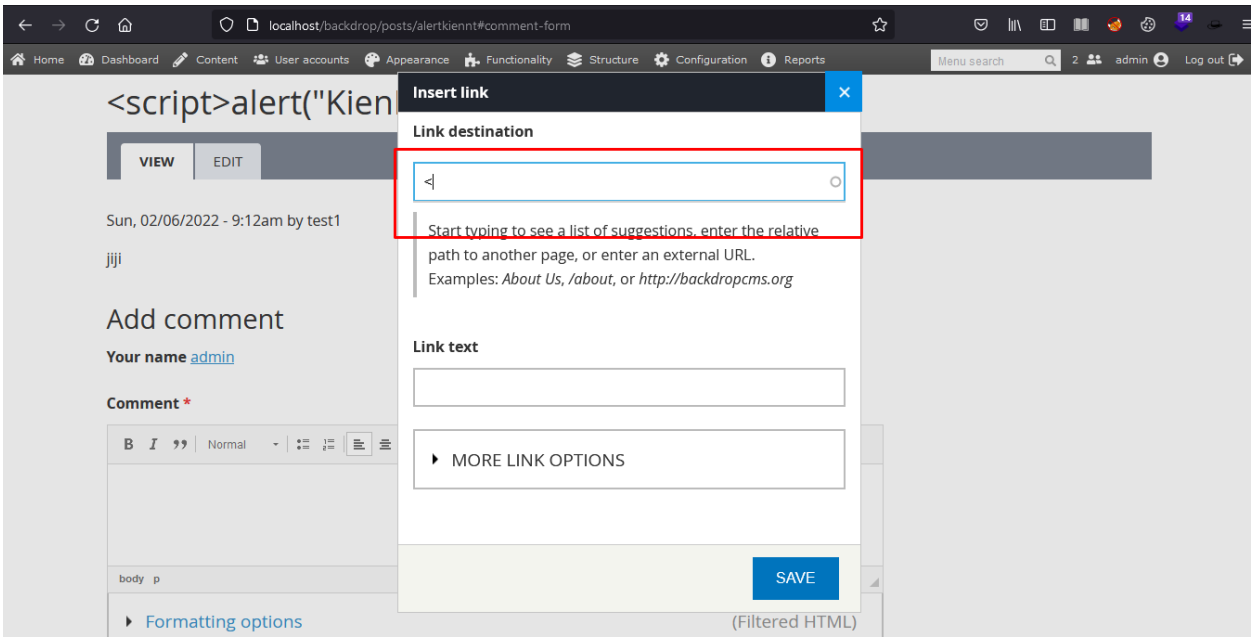


Add new post with title endpoint

In admin, join another post and comment, click add link

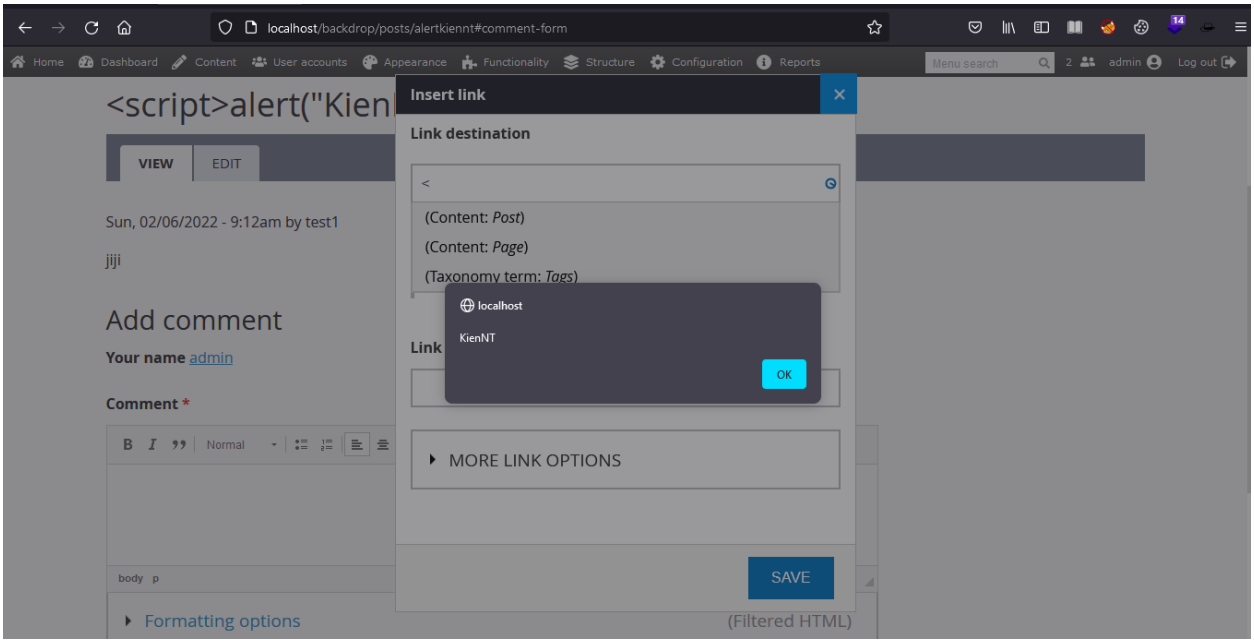


Next add `<` character

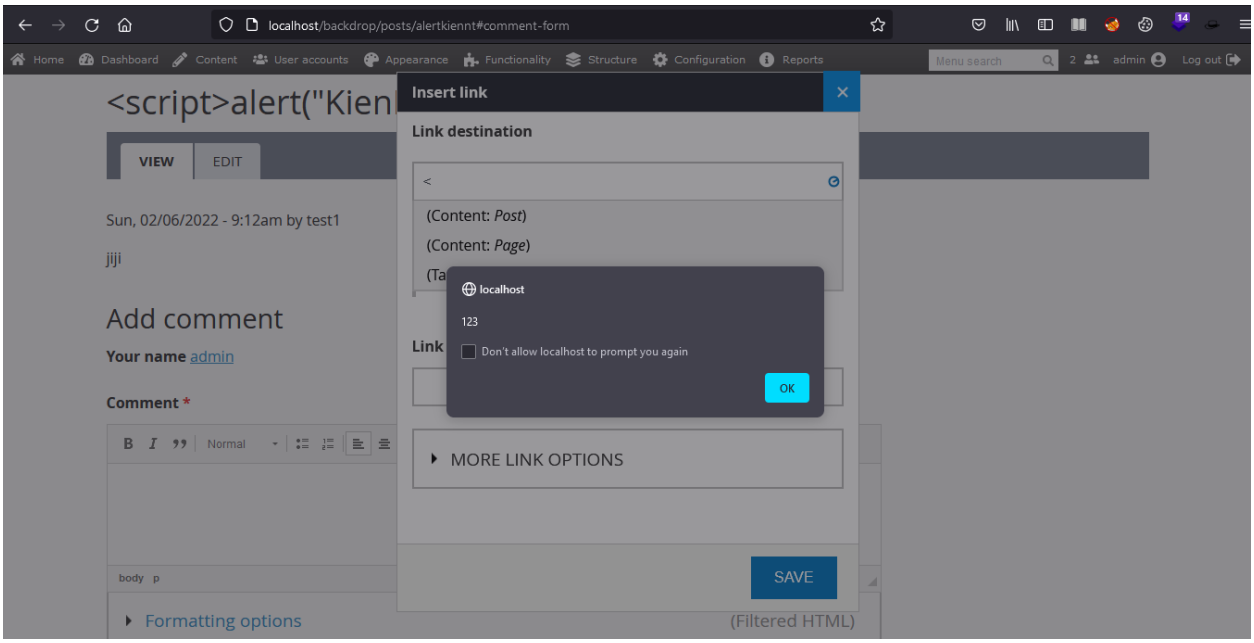


Result:

Show alert KienNT



Show alert 123



Show alert cookie