

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](mailto: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



localhost/backdrop/node/add/post

Home Dashboard Content Structure

Menu search 2 test1 Log out

Home > Add content

### Create Post

**Title \***

`<script>alert("KienNT")</script>`

**Tags**

Enter a comma-separated list of words to describe your content.

**Body (Edit summary)**

jjji

body p

Add new post with title endpoint

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

localhost/backdrop/posts/alertkientnt#comment-form

Home Dashboard Content User accounts Appearance Functionality Structure Configuration Reports

Menu search 2 admin Log out

### `<script>alert("KienNT")</script>`

**VIEW** **EDIT**

Sun, 02/06/2022 - 9:12am by test1

jjji

### Add comment

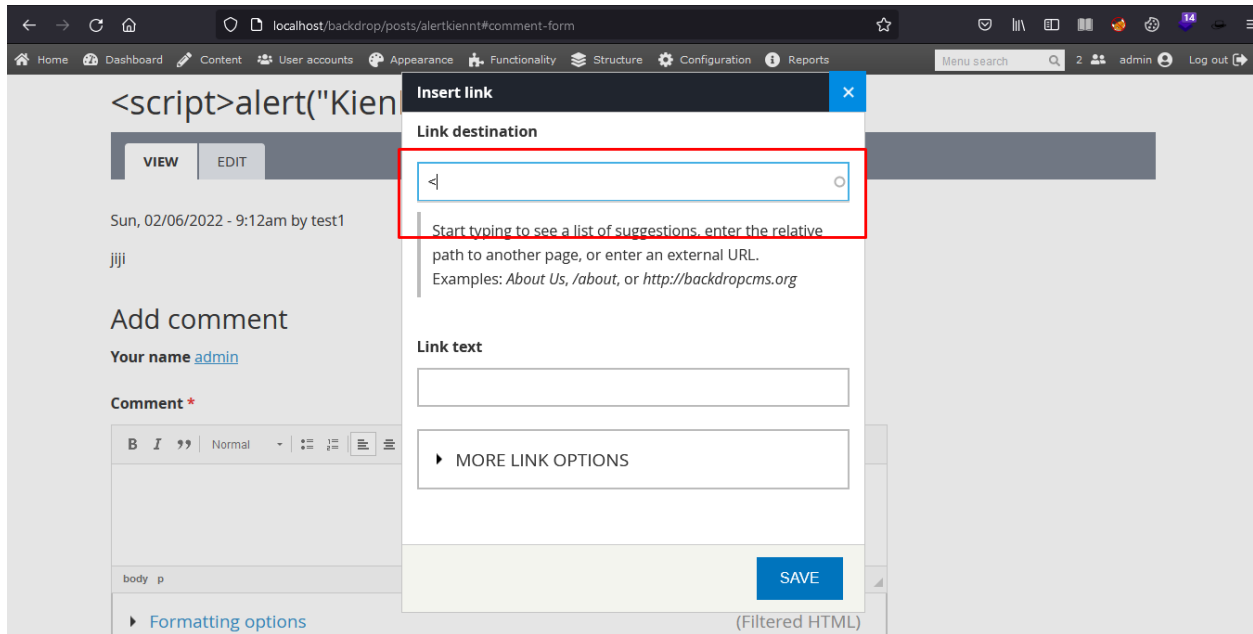
Your name [admin](#)

**Comment \***

add link

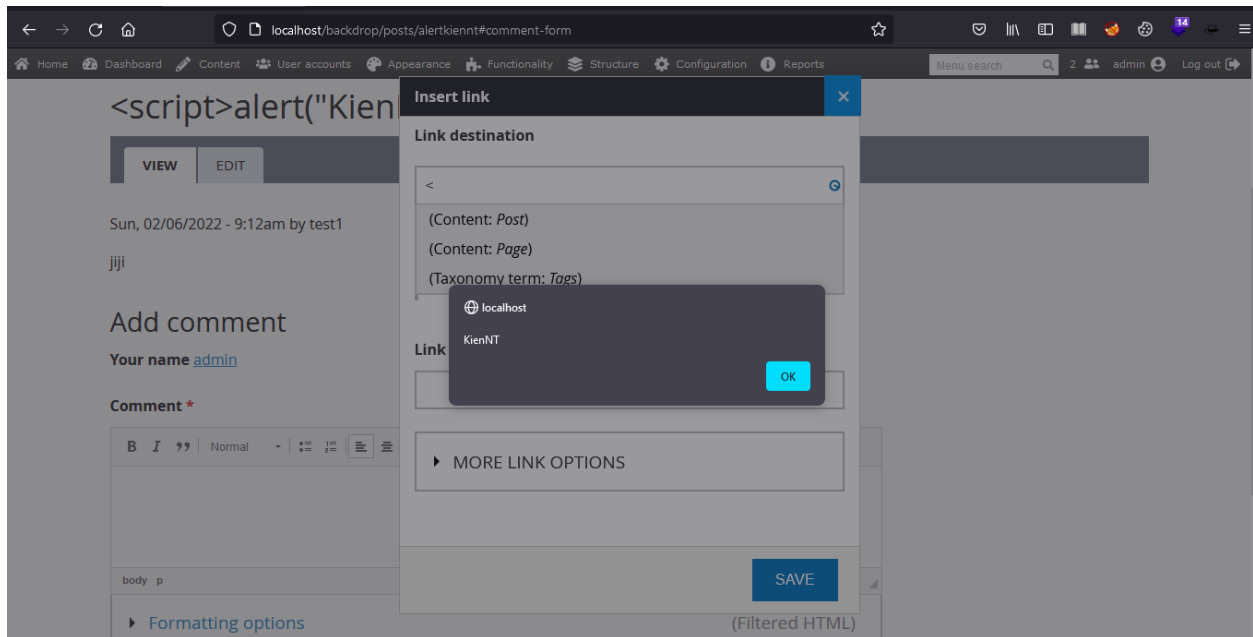
Formatting options (Filtered HTML)

Next add `` character

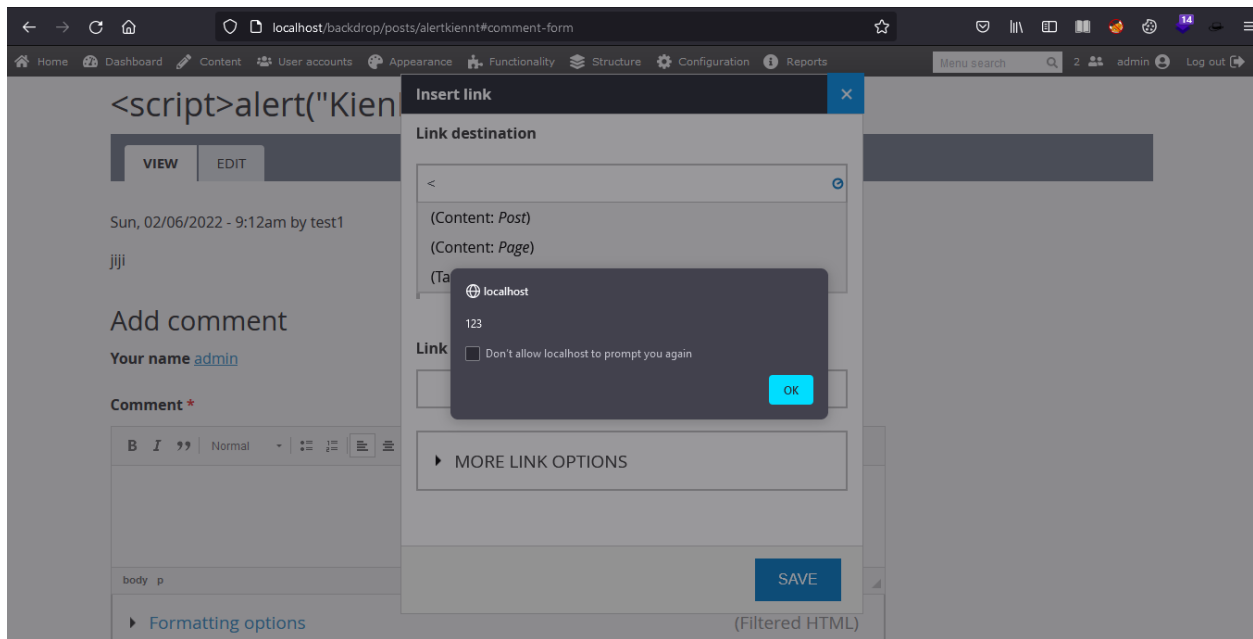


**Result:**

Show alert KienNT



Show alert 123



Show alert cookie

