



 [main](#) ▼

...

[CVE](#) / [CVE-2022-24590](#) / [CVE-2022-24590.pdf](#)

 [Nguyen-Trung-Kien](#) Add files via upload History

 1 contributor

338 KB ...

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/admin/structure/taxonomy/tags/add?destination=admin/dashboard/overview

Home > Administration > Structure > Taxonomy > Tags

### Tags: Add term

**Name \***

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

**Description**

hihi

body p

Formatting options (Filtered HTML)

**Relations**

Parent: <root>

**Parent terms**

<root>

Add new tags with name endpoint

localhost/backdrop/node/add/page

Home > Add content

### Create Page

**Title \***

`<script>alert(123)</script>`

**Body (Edit summary)**

had

body p

Formatting options (Filtered HTML)

**Publishing actions**

Publish now

**Publish action**

Add new page with title endpoint

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)**

Rich text editor toolbar: B, I, Bold, Italic, Normal, Bulleted list, Numbered list, Indent left, Indent right, Undo, Redo, Source, Link, Unlink, Image, Video, Audio, Embed, Table, Quote, Code, Preformatted, Full screen, Exit full screen.

body p

Add new post with title endpoint

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

local host/backdrop/posts/alertkiennt#comment-form

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

**VIEW** **EDIT**

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

jiji

### Add comment

Your name [admin](#)

**Comment \***

Rich text editor toolbar: B, I, Bold, Italic, Normal, Bulleted list, Numbered list, Indent left, Indent right, Undo, Redo, Source, Link, Unlink, Image, Video, Audio, Embed, Table, Quote, Code, Preformatted, Full screen, Exit full screen.

add link

Formatting options (Filtered HTML)

Next add `<` character

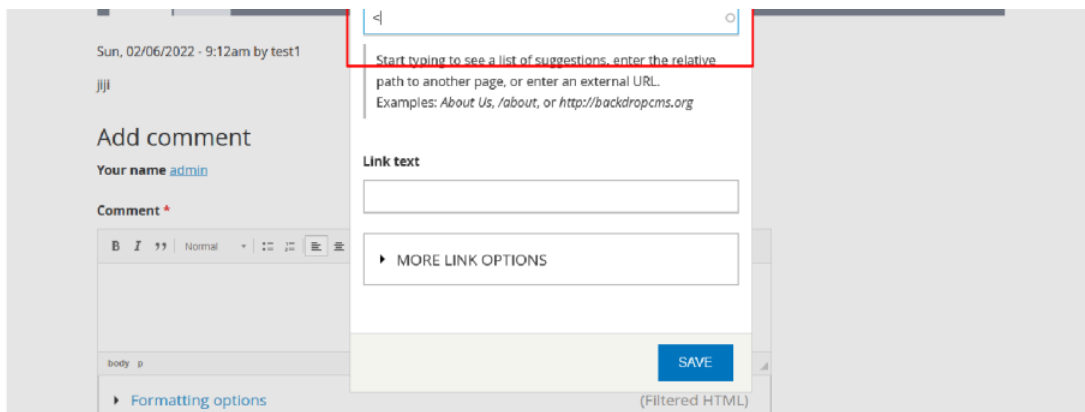
local host/backdrop/posts/alertkiennt#comment-form

## <script>alert("Kien

**VIEW** **EDIT**

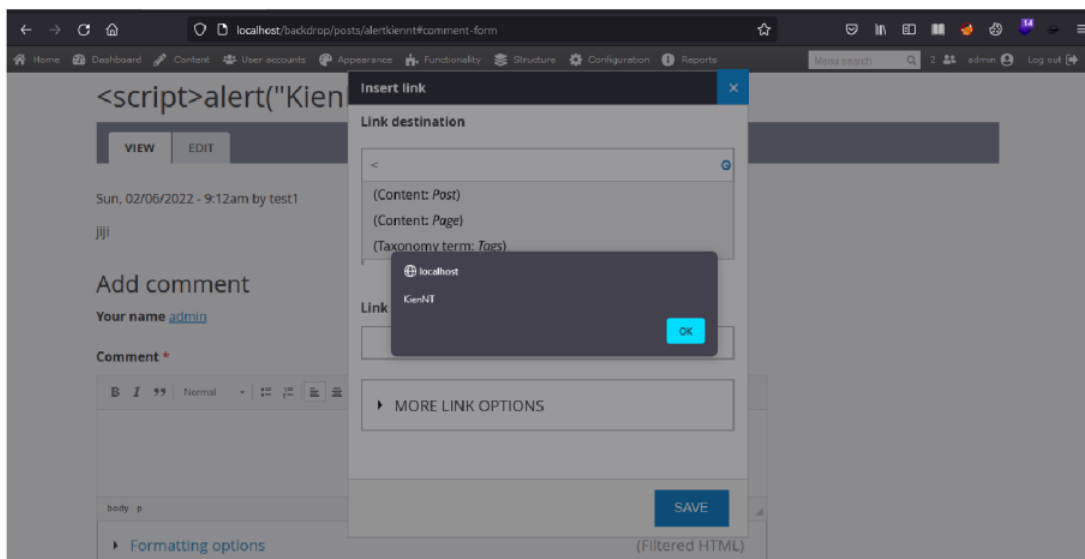
**Insert link**

Link destination

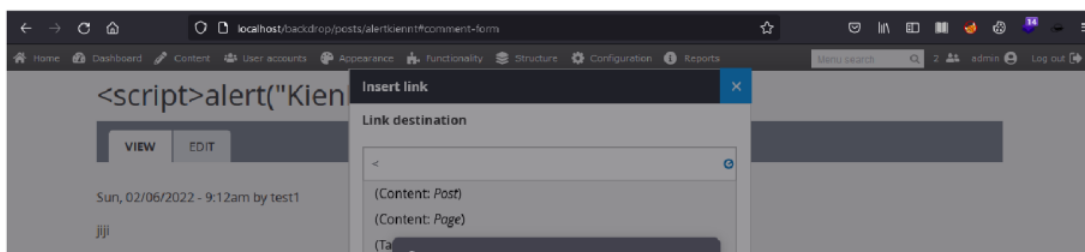


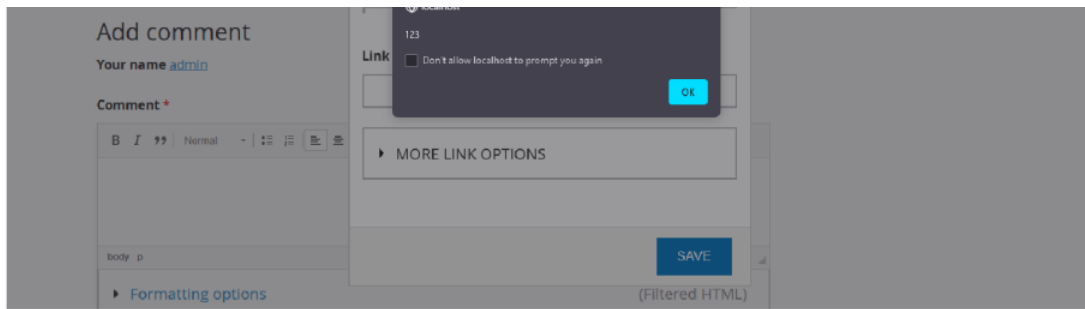
**Result:**

Show alert KienNT



Show alert 123





Show alert cookie

