

VULNERABLE: XSS store vulnerability exists in 'author' parameter in /core/admin/comment.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 'author' parameter in /core/admin/comment.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>
```

POC :

localhost/pluXml/core/admin/comment.php?c=0002.1643772360-2

Comment edit

[Back to comments](#)

Switch offline Reply to this comment Update Delete

Ip : 127.0.0.1
Status : online
Comment type : admin
Linked article : `<script>alert(6)</script>`

Date and time of publication :
02 02 2022 04:26

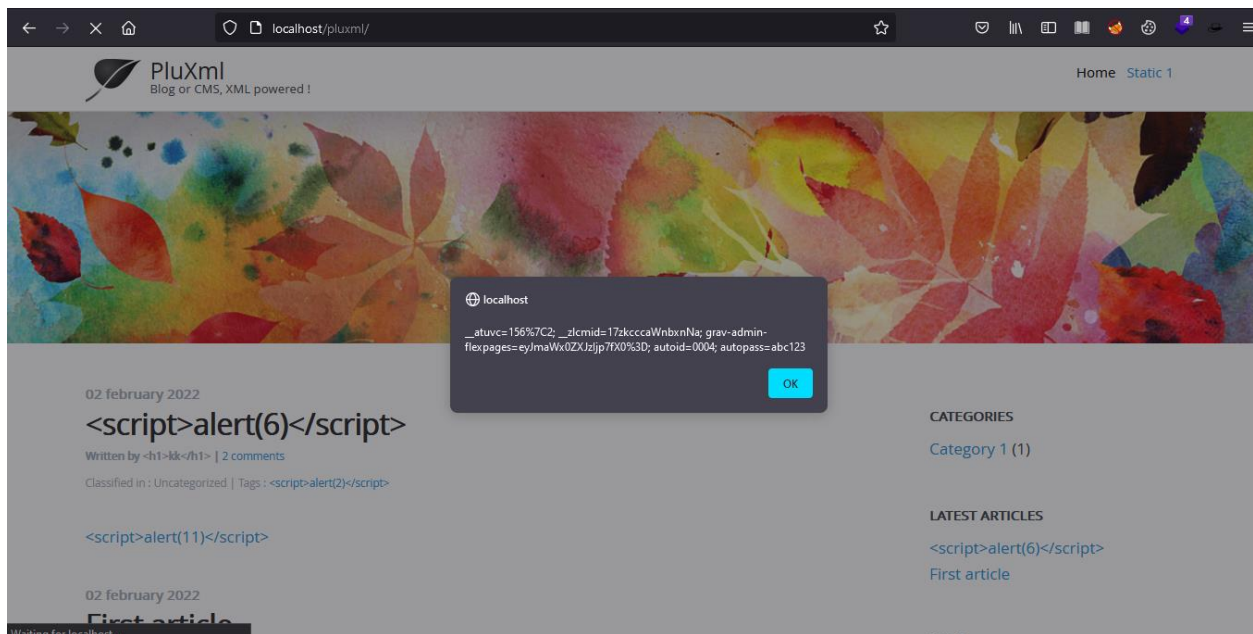
Author :
`<script>alert(document.cookie)</script>`

Site : `http://localhost/pluXml/`
`http://localhost/pluXml/`

E-mail : `1@gmail.com`
`1@gmail.com`

Comments :
`xin chao`

Result:



Show Alert

File Affect: /core/admin/comment.php

```

<div class="grid">
  <div class="col sml-12">
    <label for="id_author"><?php echo L_COMMENT_AUTHOR_FIELD ?> :</label>
    <?php plxUtils::printInput('author',$author,'text','40-255') ?>
  </div>
</div>

```