



 [main](#) ▼

...

[CVE](#) / [CVE-2022-24585](#) / [CVE-2022-24585.pdf](#)

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

 1 contributor

231 KB ...

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: [nguyentruengkien.31120@gmail.com](mailto:nguyentruengkien.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

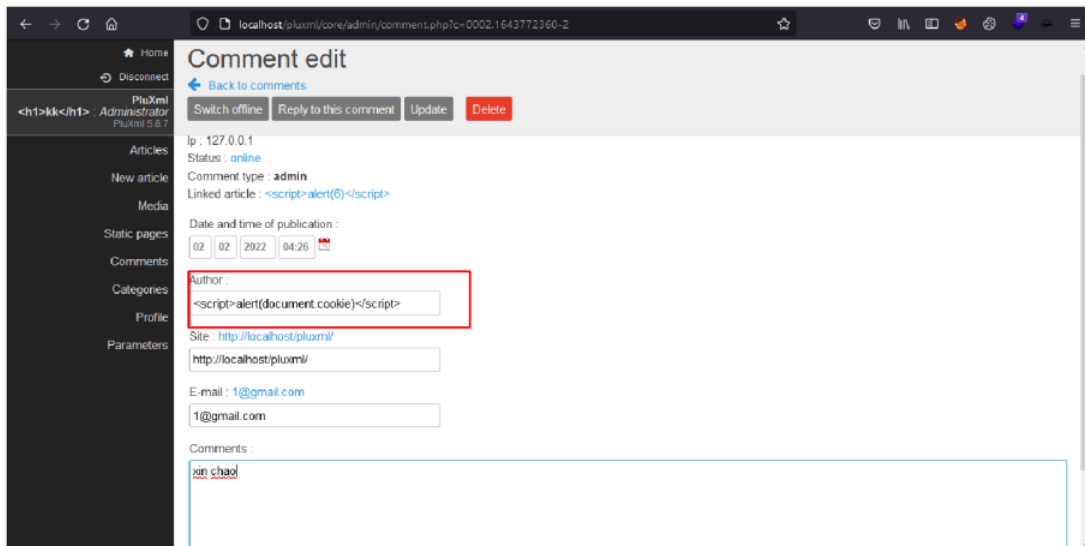
**Impact:** Attackers can masquerade as authorized users via session cookies, allowing them to perform any action allowed by the user account.

**Suggestions:** User input should be filter, Escaping

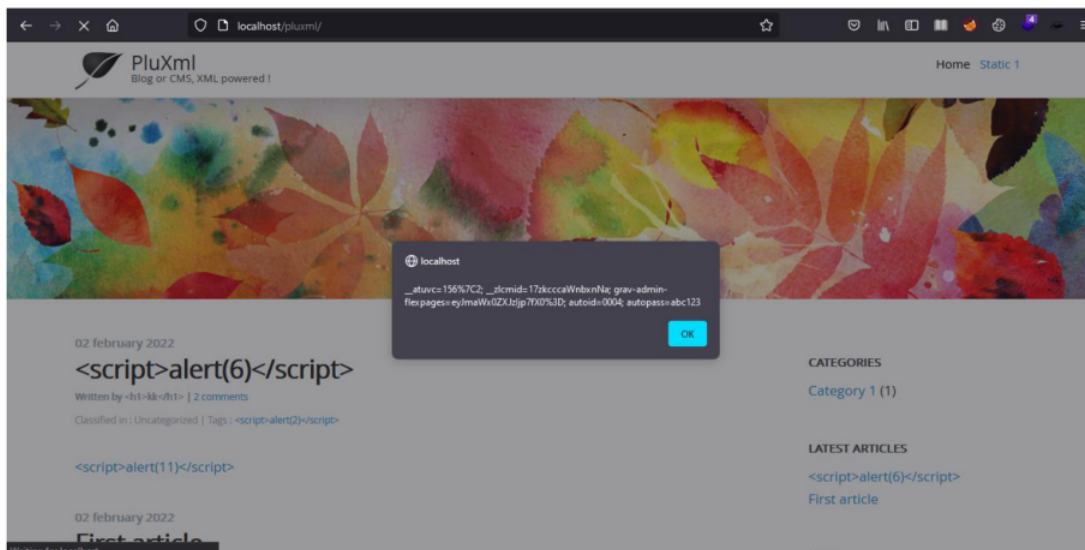
**Payload :**

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

**POC :**



Result:



Show Alert

File Affect: /core/admin/comment.php

