




 [main](#) ▼

...

[CVE](#) / [CVE-2022-24227](#) / [CVE-2022-24227.pdf](#)

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

 History

 1 contributor

225 KB ...

VULNERABLE: XSS store vulnerability exists in 'name' and 'last' parameter Boltwire version 7.10 allows attackers to execute arbitrary web scripts or HTML

Date: 01/30/2022

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:** Boltwire v7.10

Vendor : [www.boltwire.com](http://www.boltwire.com)

Description : XSS store vulnerability exists in 'name' and 'last' parameter Boltwire version 7.10 allows attackers to execute arbitrary web scripts or HTML

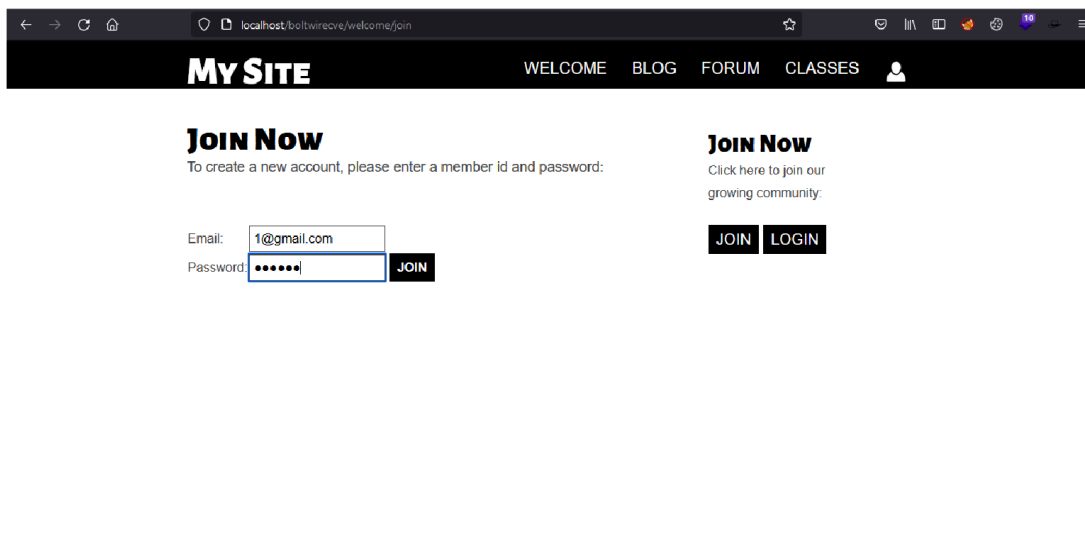
Impact: Attackers can masquerade as authorized users via session cookies, allowing them to perform any action allowed by the user account.

Suggestions: User input should be filter, Escaping

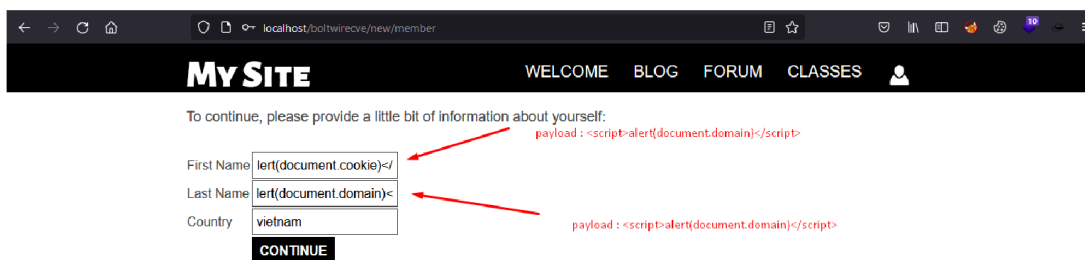
Payload :

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

POC:



Register new user

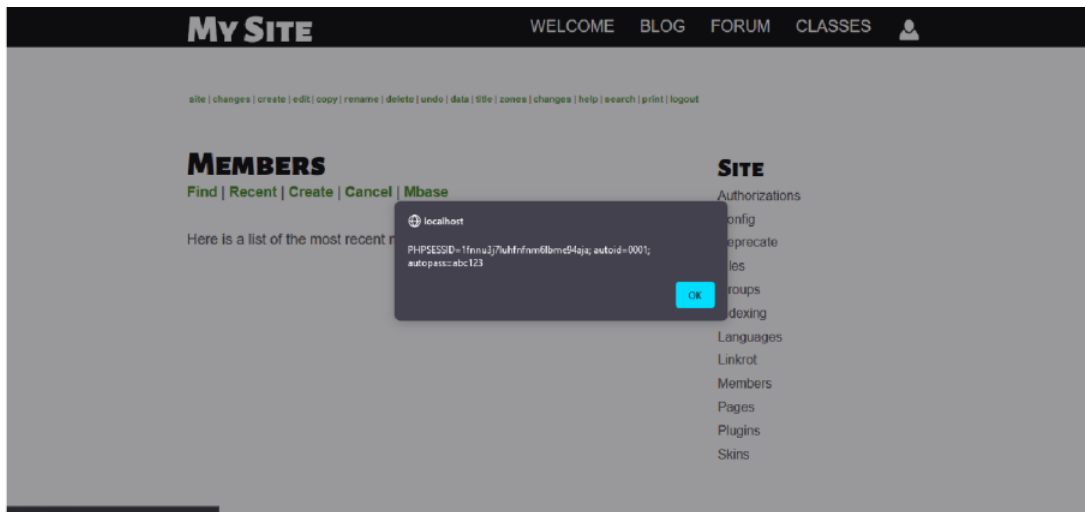


Add payload in 2 endpoint

**Result:** In admin, when admin view member list, it show alert

Alert cookie





## Alert domain

