




 [main](#) ▼

...

[CVE](#) / [CVE-2022-24589](#) / [CVE-2022-24589.pdf](#)

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

 History

 1 contributor

229 KB ...

VULNERABLE: XSS store vulnerability exists in 'task' parameter and add Category function in Burden version 3.0 allows attackers to execute arbitrary web scripts or HTML

Date: 02/04/2022

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: Burden v3.0

Vendor : Josh Fradley burden

Description : XSS store vulnerability exists in 'task' parameter and add Category function in Burden version 3.0 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.

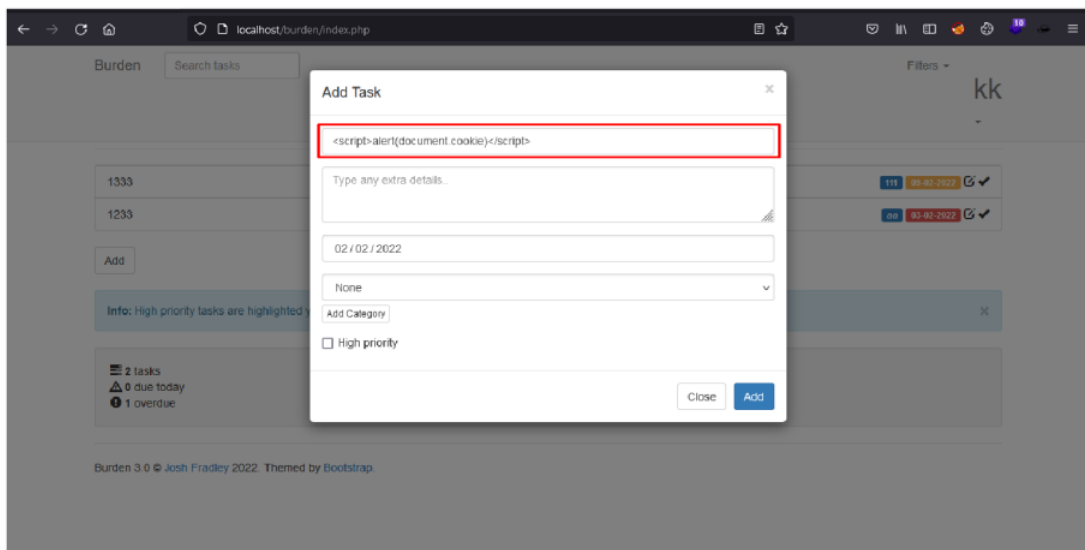
Suggestions: User input should be filter, Escaping

Payload :

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

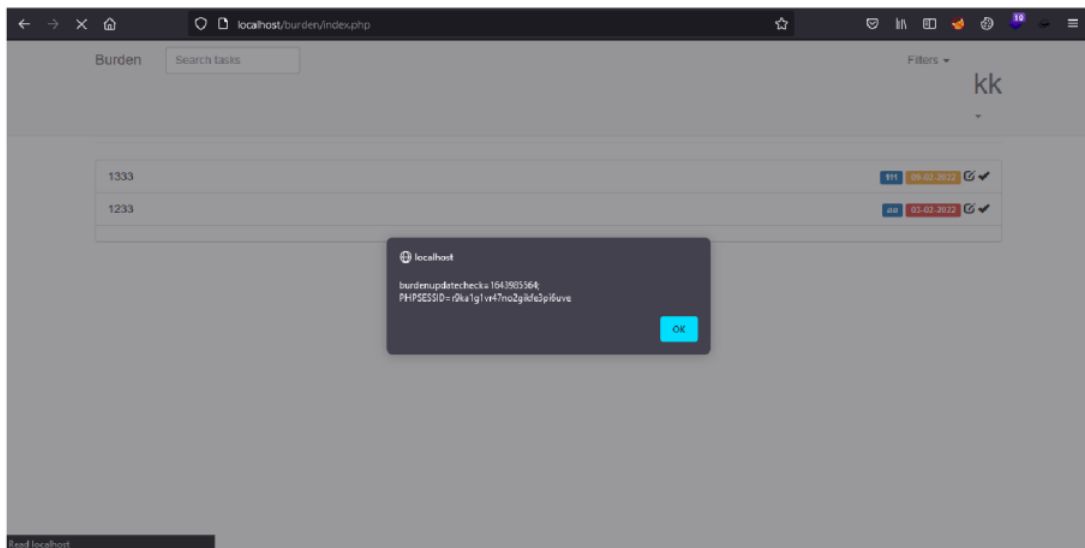
POC:

In task parameter

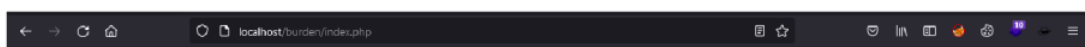


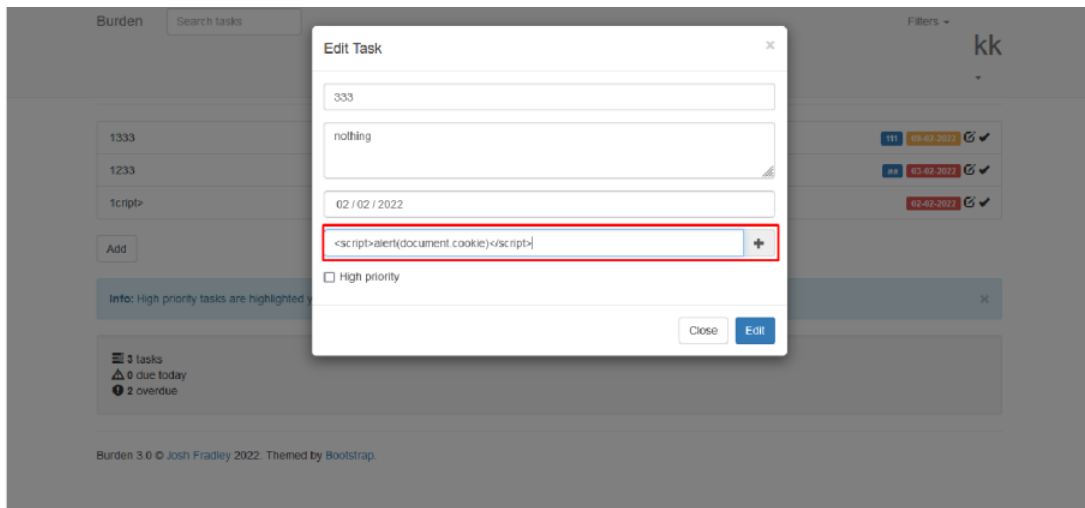
Result:

Alert cookie



In add category





Result:

Show alert

