New issue

Jump to bottom

XSS issue in the "Text" parameter (forums) #6194

Closed trungtin1998 opened this issue on Mar 20 · 4 comments

Assignees

Labels bug

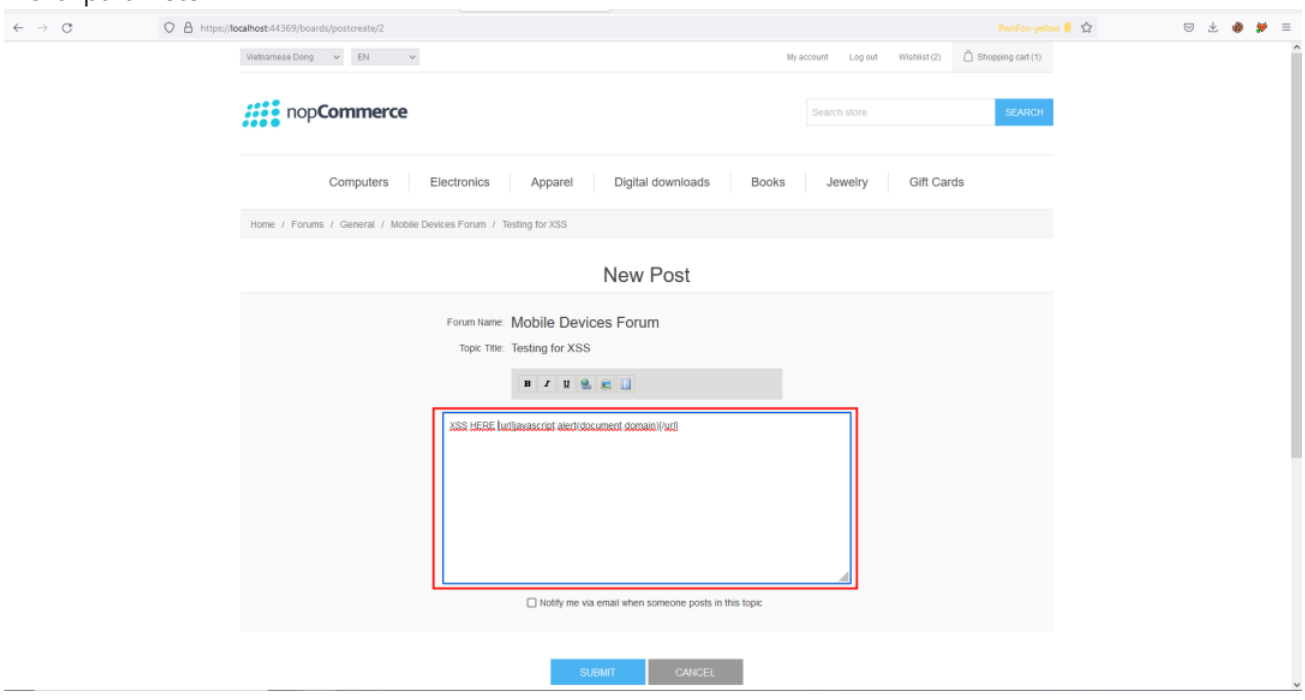
Milestone Version 4.60

trungtin1998 commented on Mar 20 • edited

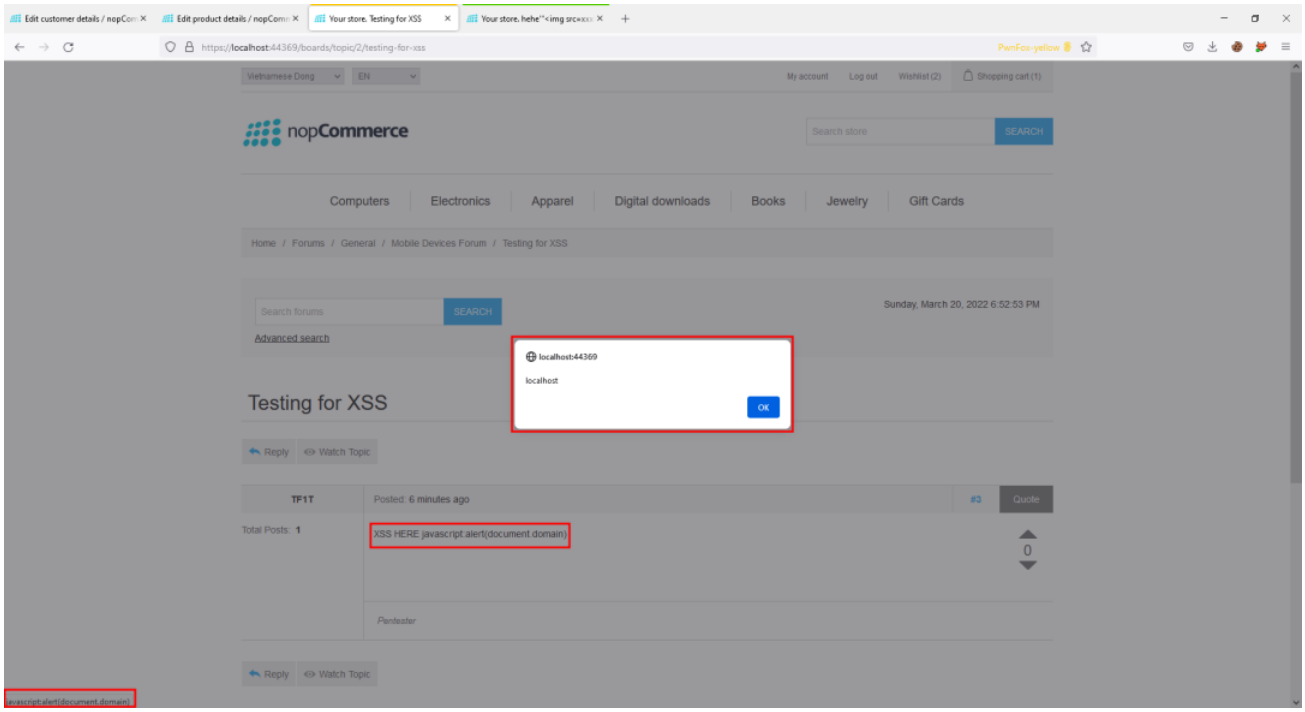
nopCommerce version: 4.50.1

Description: A stored cross-site scripting (XSS) vulnerability exists when creating a new post of nopCommerce version 4.50.1 that allows a remote attacker to execute arbitrary JavaScript code at client browser
Steps to reproduce the problem:

- Step 1: Create new topic or reply topic with injecting `[url]javascript:alert(document.domain)[/url]` to "Text" parameter



- Step2: Click a text `javascript:alert(document.domain)` at topic that was created in step 1 to trigger XSS



Let me know if you require additional information.

AndreiMaz added this to the **Version 4.60** milestone on Mar 20

AndreiMaz added the **discussion / investigation** label on Mar 20

AndreiMaz assigned **skoshelev** on Mar 20

AndreiMaz changed the title ~~XSS issue in the "Text" parameter~~ **XSS issue in the "Text" parameter (forums)** on Mar 20

skoshelev commented on Mar 21 — Contributor

Hi **@trungtin1998**. Thank you for your help. We fixed this problem by this commit

skoshelev closed this as completed on Mar 21

---

skoshelev added bug and removed **discussion / investigation** labels on Mar 21

trungtin1998 commented on Mar 21 Author

Hi guys, Can you help me request CVE for this issue?

AndreiMaz commented on Mar 22 Member

@trungtin1998 Please feel free to report it at https://www.cve.org/

But our team will appreciate if you do after the next version release of nopCommerce (we plan to release a minor version in April)

trungtin1998 commented on Mar 22 Author

Hi **@AndreiMaz**, thank you for your information. I will do it after the next version release of nopCommerce.

Assignees

skoshelev

Labels

bug

Projects

None yet

Milestone

Version 4.60

Development

No branches or pull requests

3 participants