New issue

Jump to bottom

Stored XSS in customer name when customer accessed deny resource and redirect to login page #6191

Closed trungtin1998 opened this issue on Mar 19 · 1 comment

Assignees

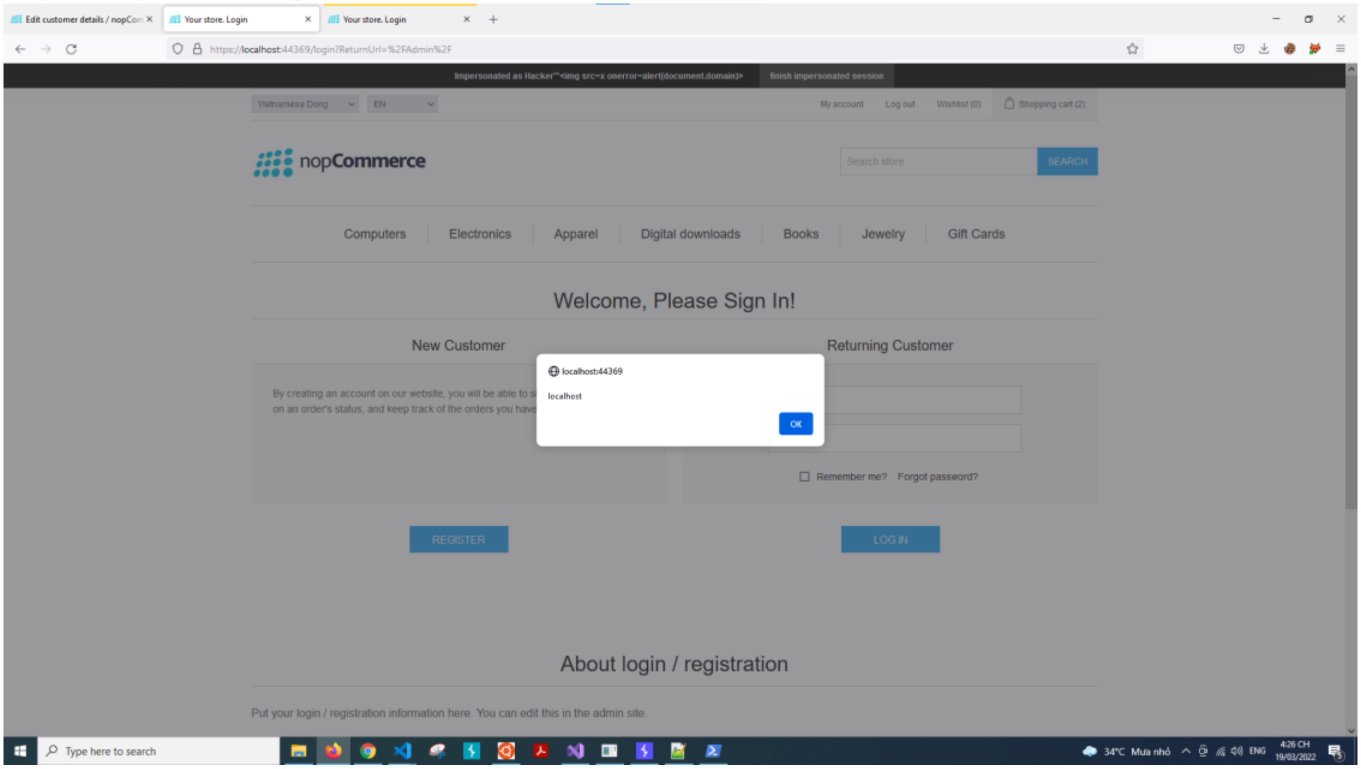
Labels bug

Milestone Version 4.60

trungtin1998 commented on Mar 19

nopCommerce version: 4.50.1

Steps to reproduce the problem:



https://localhost:44369/login?ReturnUrl=%2FAdmin%2F

Impersonated as Hacker"'<img src=x onerror=alert(document.domain)>

Welcome, Please Sign In!

By creating an account on our website, you will be able to s… on an order's status, and keep track of the orders you have…

localhost:44369

localhost

About login / registration

Put your login / registration information here. You can edit this in the admin site.

- Inject javascript code to First name or Last name at Customer Info

- When customer accesses deny resources, for example /admin, server will redirect user to login page and show up notification: "You are already logged in as {Customer Name}. You may log in with another account.". Customer Name is reflected in the response without HTML encoding, and cause XSS when displayBarNotification() is called.
  Note: If admin used Place order (impersonate) feature, customer will execute javascript under admin session.

AndreiMaz added this to the **Version 4.60** milestone on Mar 19

AndreiMaz added the **discussion / investigation** label on Mar 19

AndreiMaz assigned **skoshelev** on Mar 19

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

skoshelev commented on Mar 22 Contributor

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

Closed #6191

skoshelev closed this as completed on Mar 22

Assignees

skoshelev

Labels

bug

Projects

None yet

Milestone

Version 4.60

Development

No branches or pull requests

3 participants