

[New issue](#)

[Jump to bottom](#)

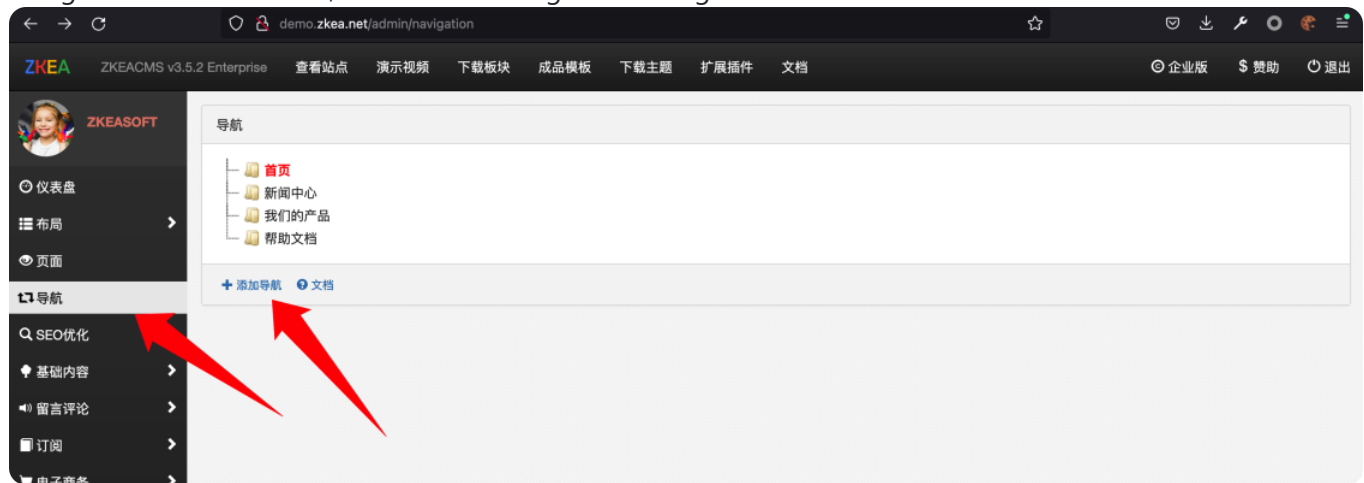
There is XSS vulnerability that can be able to obtain sensitive user information in the foreground #457

✓ Closed NKingpp opened this issue on Apr 11 · 1 comment

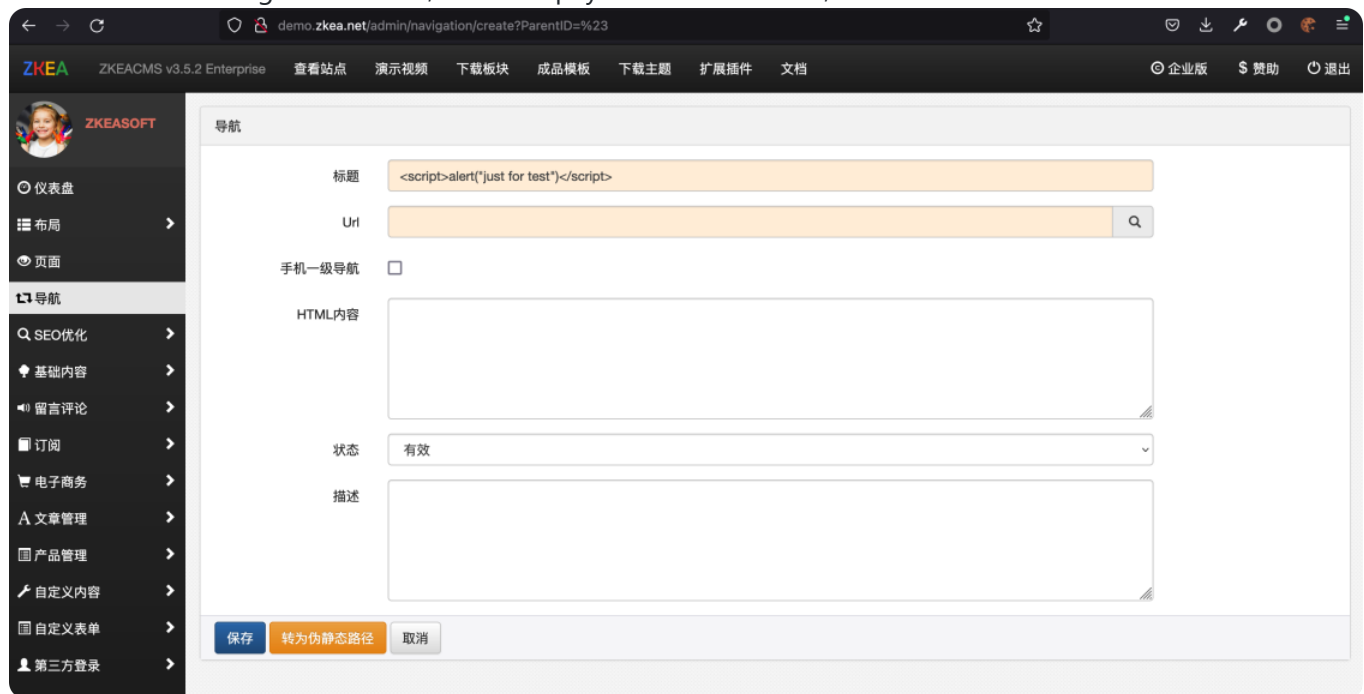
NKingpp commented on Apr 11

Reproduction process

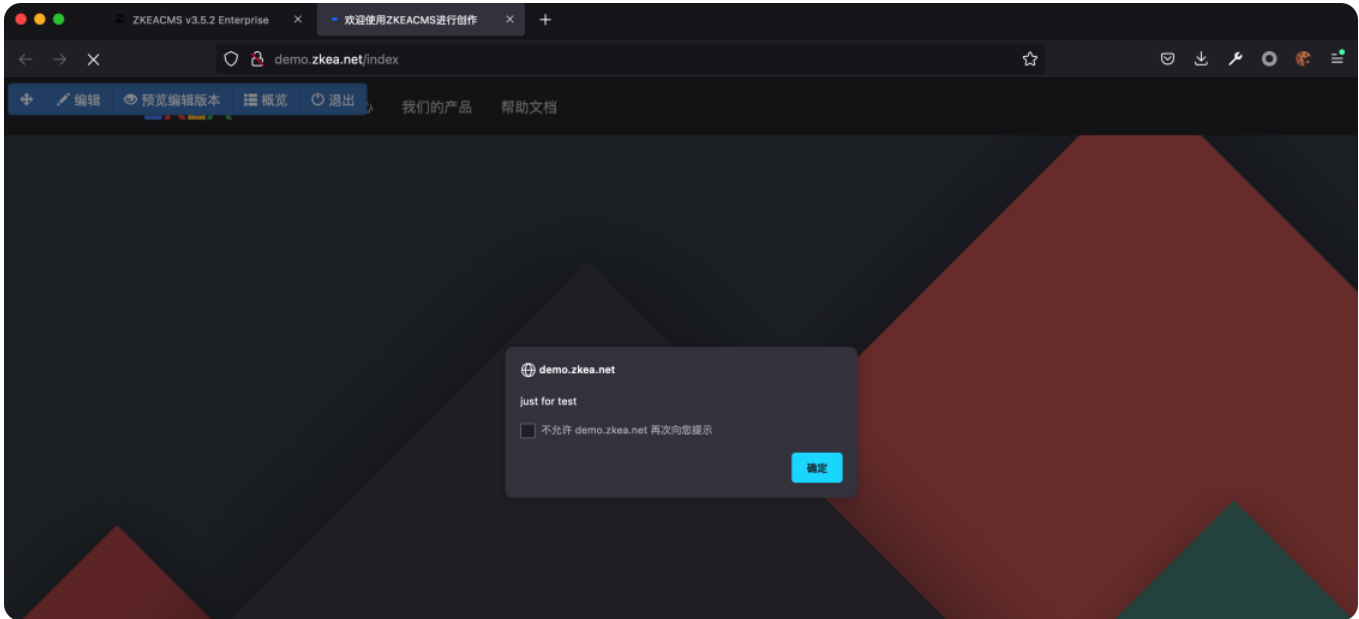
1. Log in to the back office, Click on the background navigation function.



2. Click the Add Navigation button, Insert xss payload in the header, As shown below.



3. Then click save and go back to the front page of the cms to trigger the xss vulnerability.



Restoration suggestions

- 1.Backend filters input for pointed brackets.
- 2.Frontend uses html entity coding output.



SeriaWei commented on Apr 11


Owner

Thanks for the feedback, we will fix it in the next release.

 SeriaWei added a commit that referenced this issue on Apr 14

 Sanitize Html ...

✓ 833c546

 SeriaWei closed this as completed on May 1

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

