

New issue

[Jump to bottom](#)

## XSS via modul post loop in Pages #525

Open gozan10 opened this issue 21 days ago · 0 comments

gozan10 commented 21 days ago • edited ▼

Hi team,

I find XSS via modul post loop in Pages

Step:

1. add section in manage sections

The image displays two screenshots of the WBCE CMS 'Manage Sections' interface, illustrating the process of adding a new section.

**Top Screenshot:** The 'Manage Sections' page is shown. The 'Add Section' button is highlighted with a red box. The table below shows one existing section:

Type	Block	Section Name	Start date	End date	ID
WYSIWYG	Content	abc	01.01.1970 00:00	01.01.1970 00:00	2

**Bottom Screenshot:** The 'Manage Sections' page is shown after adding a new section. The 'News with Images' section is highlighted with a red box. The table now contains two sections:

Type	Block	Section Name	Start date	End date	ID
WYSIWYG	Content	abc	01.01.1970 00:00	01.01.1970 00:00	2
News with Images	Content				8

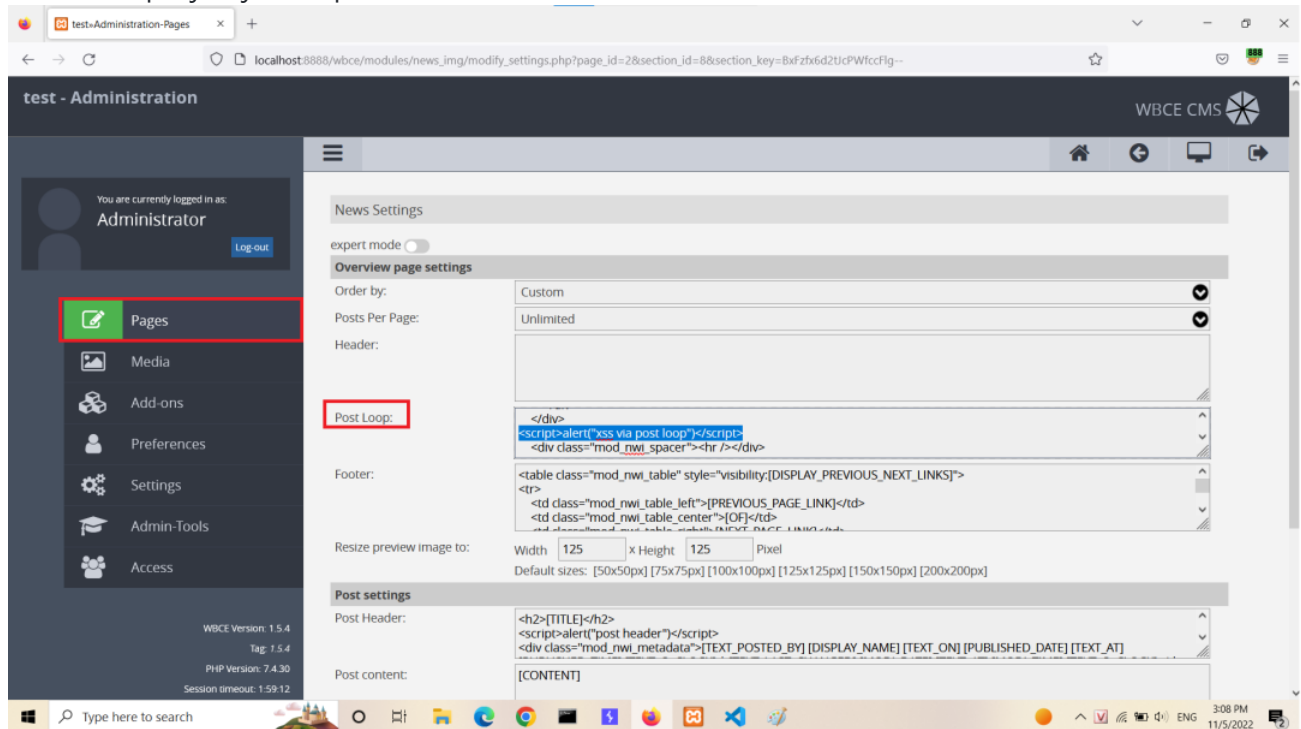
2. add new post then choose options in modify page (a new post must be created for the setting to take effect)

The first screenshot shows the WBCE CMS administration interface. The left sidebar contains a menu with the following items: Pages (highlighted with a red box), Media, Add-ons, Preferences, Settings, Admin-Tools, and Access. The main content area displays the 'Block: Content Modul: News with Images ID: 8 Name:' section. Below this, there are tabs for 'Posts' and 'Groups'. The 'Options' tab is highlighted with a red box. The 'Import Section' is set to 'Section 5'. The bottom status bar shows 'WBCE Version: 1.5.4', 'Tag: 1.5.4', 'PHP Version: 7.4.30', and 'Session timeout: 1:59:51'.

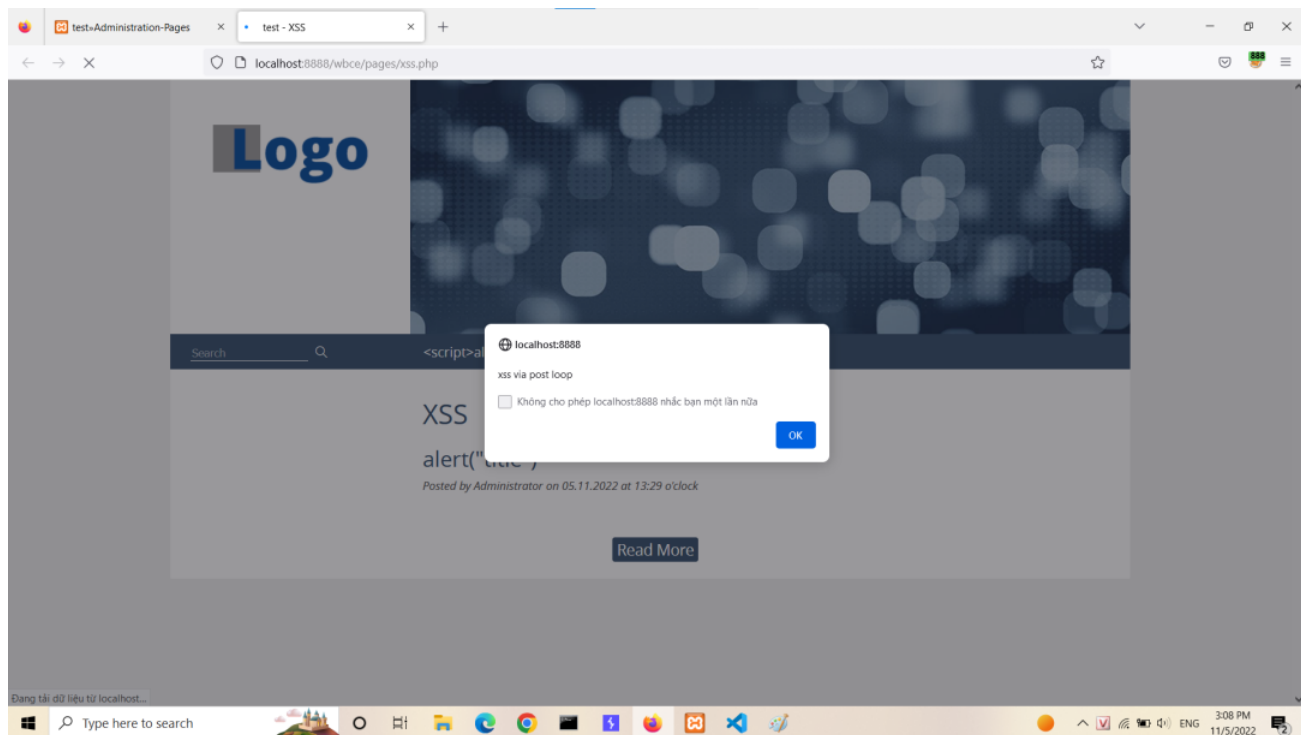
The second screenshot shows the same interface after a new post has been added. The 'Posts' tab is selected, and a table of posts is displayed. The table has the following columns: Title, Group, Active, Tags, Start date, and End date. A red box highlights the first row of the table, which contains the following data: Title: ad, Group: (empty), Active: (checked), Tags: 0, Start date: 05.11.2022 15:10, and End date: (empty). Below the table, the text 'impact in new post' is visible. The bottom status bar shows 'WBCE Version: 1.5.4', 'Tag: 1.5.4', 'PHP Version: 7.4.30', and 'Session timeout: 1:56:28'.


Title	Group	Active	Tags	Start date	End date
ad		<input checked="" type="checkbox"/>	0	05.11.2022 15:10	

### 3. In Post Loop inject javascript



### 4. save and view



 instantflorian added a commit that referenced this issue 12 days ago

 NWISettings settings for admins only (optional) ...

26b9c1a

Assignees

No one assigned

---

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

1 participant

