

New issue

[Jump to bottom](#)

Cross Site Script Vulnerability on module "Shop" in NavigateCMS 2.9 #10

🔒 Closed r0ck3t1973 opened this issue on Jun 17, 2020 · 2 comments

r0ck3t1973 commented on Jun 17, 2020 • edited

/Describe the bug/

An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Shop" feature Navigate

/To Reproduce/

Steps to reproduce the behavior:

1. Login into the panel
2. Go to 'navigate/navigate.php?fid=dashboard'
3. Go to Module "Shop"
4. Chose:
 - Go to "/navigate/navigate.php?fid=products"
 - Go to "/navigate/navigate.php?fid=coupons"
 - Go to "/navigate/navigate.php?fid=brands"
 - Go to "/navigate/navigate.php?fid=shipping_methods"
 - Go to "/navigate/navigate.php?fid=payment_methods"

5. Click "Create" >> Insert Payload:

'><details/open/ontoggle=confirm(1337)>

6. Save: XSS alert Message!

/Expected behavior/

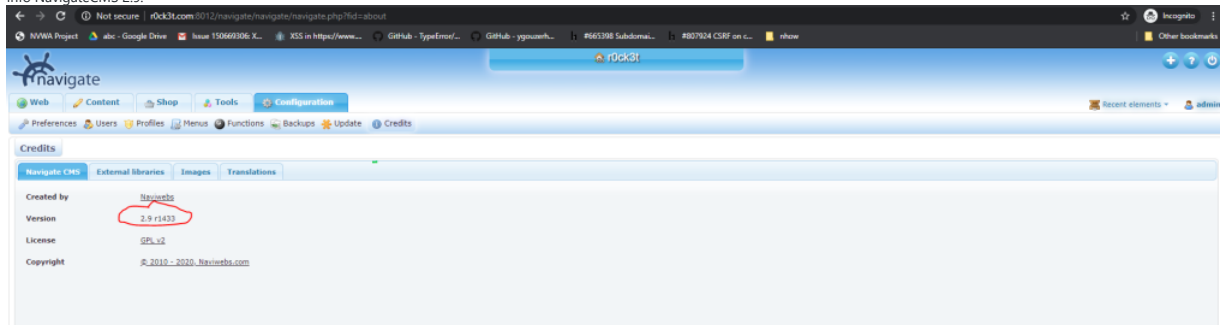
The removal of script tags is not sufficient to prevent an XSS attack. You must HTML Entity encode any output that is reflected back to the page

/Impact/

Commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

/Screenshots/

Info NavigateCMS 2.9:



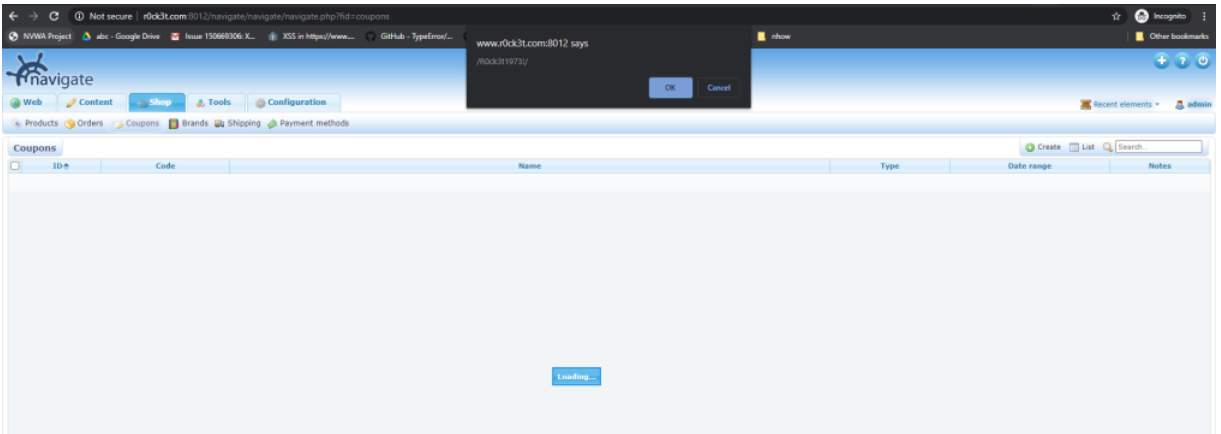
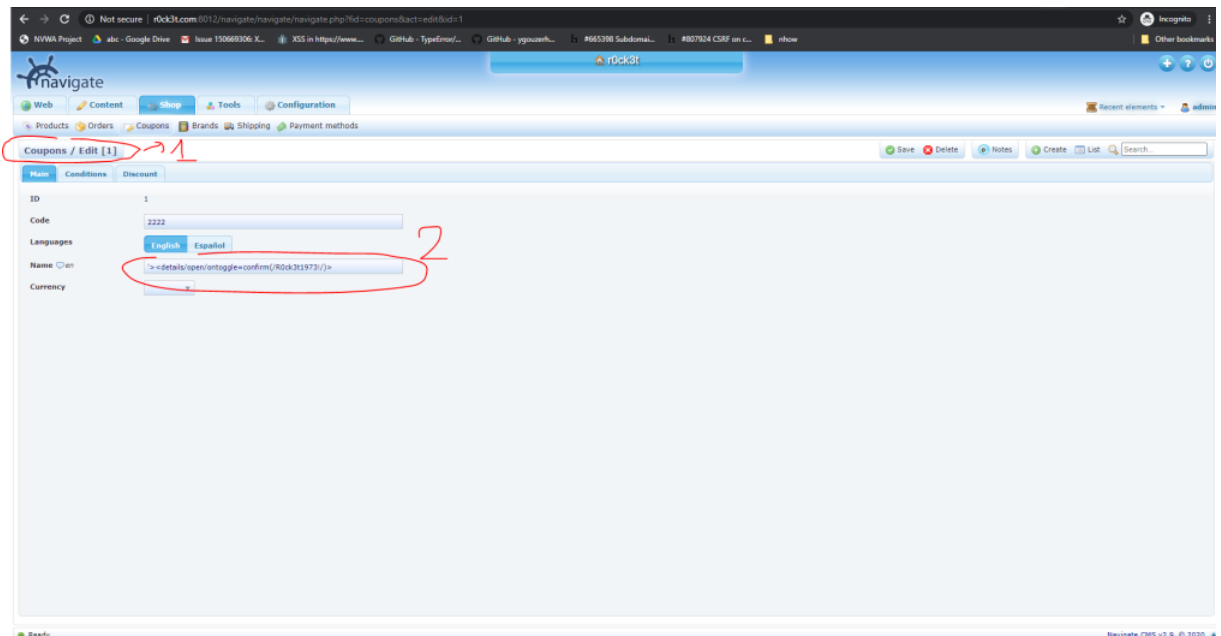
Ex1: Chose go to: "/navigate/navigate.php?fid=products"

The first screenshot shows the main CMS dashboard with the 'Products' menu item circled in red and labeled '2'. The 'Create' button in the top right is also circled in red and labeled '3'. The 'Show' button in the top navigation bar is circled in red and labeled '1'.

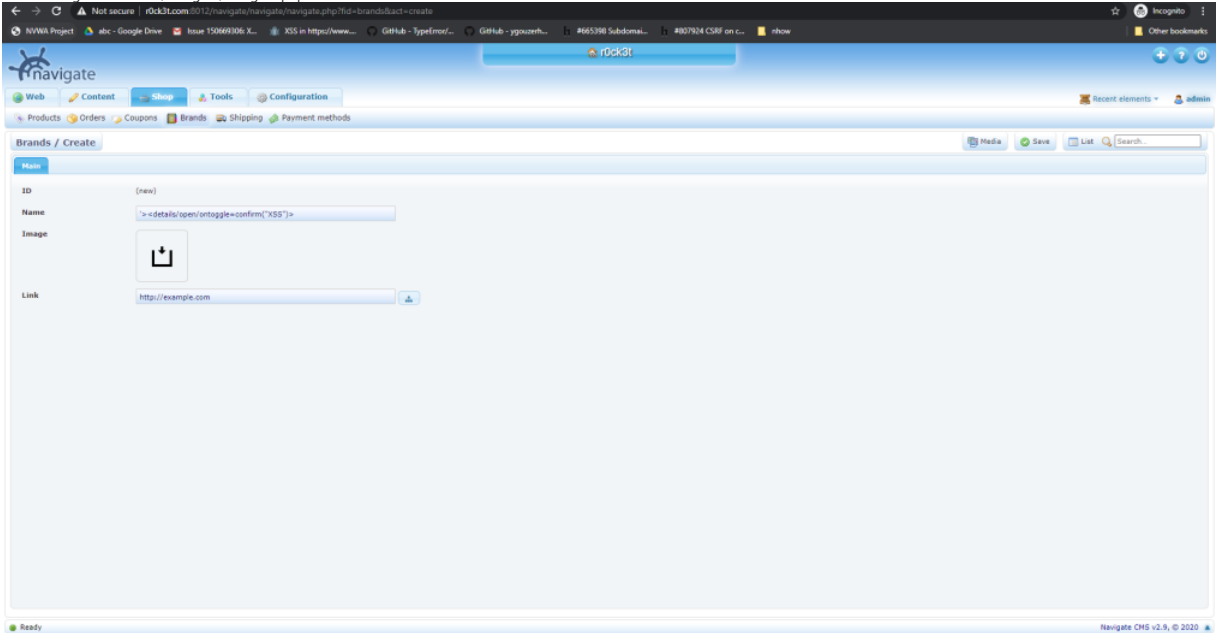
The second screenshot shows the 'Products / Edit [2]' form. The 'Title' field contains the payload: `<=details/open/ontoggle=confirm(1337)>`. The 'Path' field contains: `/home/>=details/open/ontoggle=confirm(1337)>`. The 'Main content' area contains the text 'test'.

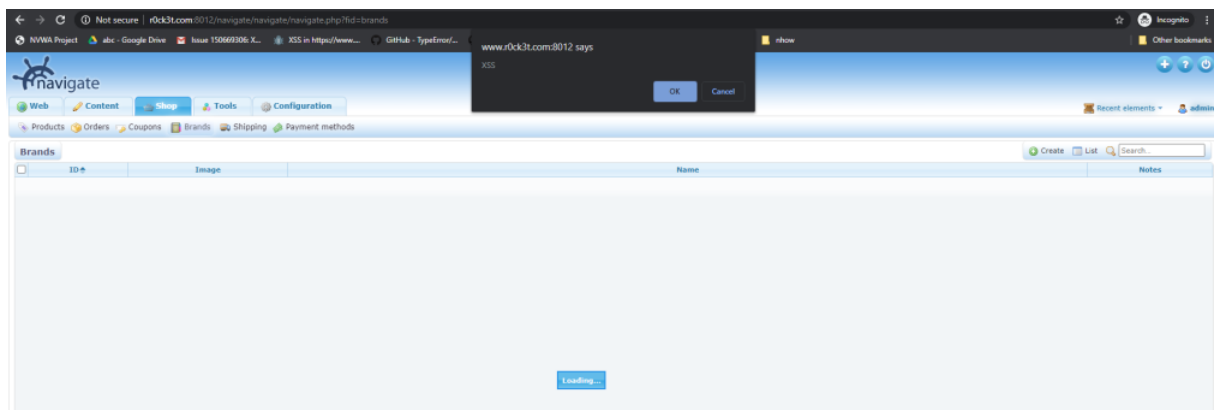
The third screenshot shows the CMS interface after the product is added. A modal dialog box is displayed with the text 'www.r0ck3t.com:8012 says 1337' and 'OK' and 'Cancel' buttons. The 'Products' table at the bottom shows a 'Loading...' status.

Ex2: Chose go to: "/navigate/navigate.php?fid=coupons"

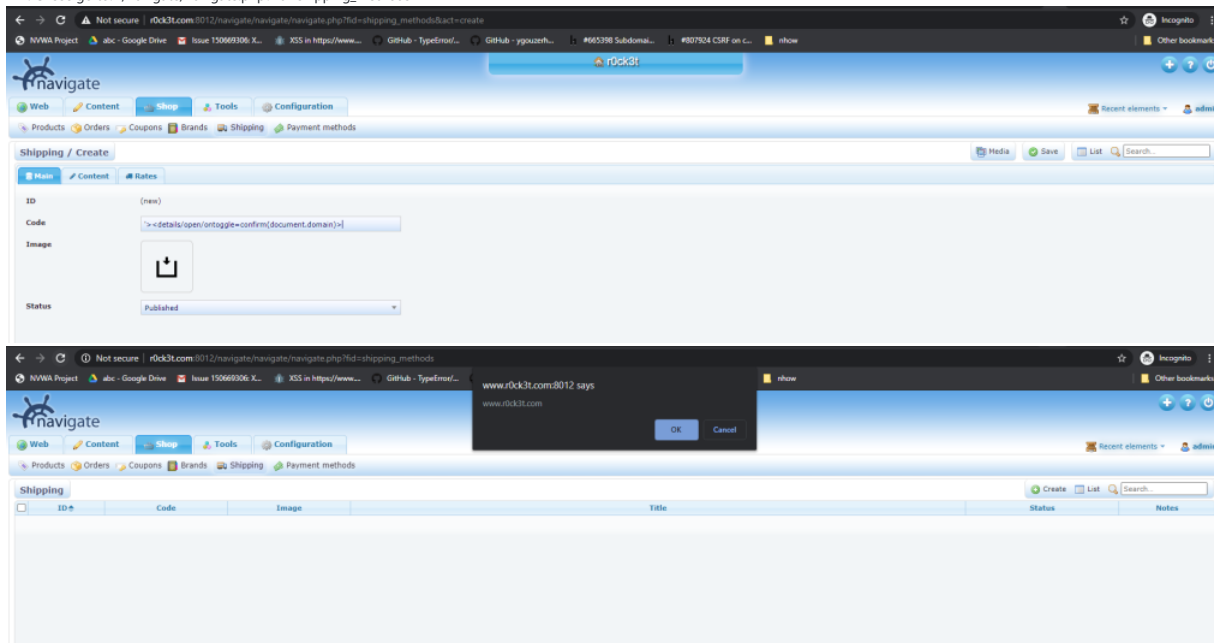


Ex3: Chose go to: "Go to "/navigate/navigate.php?fid=brands"

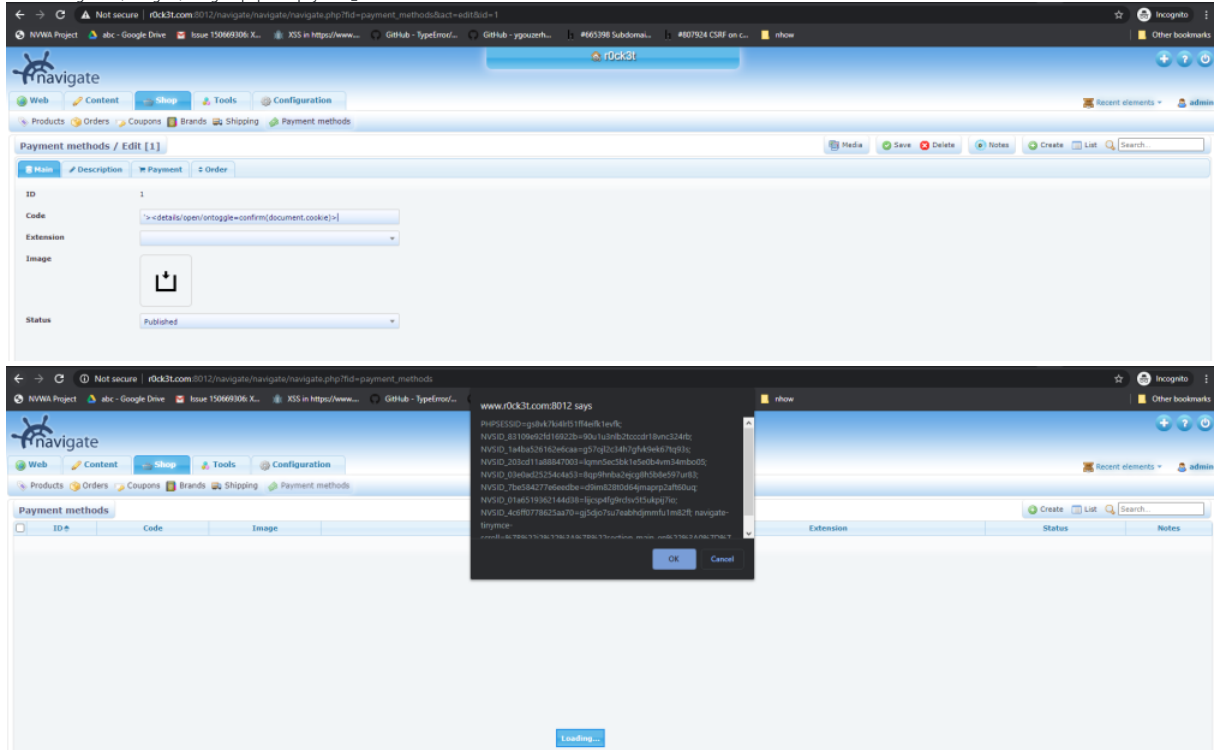




Ex4: Chose go to: "/navigate/navigate.php?fid=shipping_methods"



Ex5: Chose go to: "/navigate/navigate.php?fid=payment_methods"



/Desktop (please complete the following information)/
OS: Windows
Browser: All


I Hope you fix it ASAP

  r0ck3t1973 changed the title ~~Cross Site Script Vulnerability on "Shop" in NavigateCMS 2.9~~ Cross Site Script Vulnerability on module "Shop" in NavigateCMS 2.9 on Jun 17, 2020

NavigateCMS commented on Jun 18, 2020

Owner

Fixed by commit [9be8944](#)

 NavigateCMS closed this as completed on Jun 18, 2020

r0ck3t1973 commented on Jun 18, 2020

Author

Hi Team Security NavigateCMS

You can a CVE ID assign!

Thanks you!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

