

New issue

[Jump to bottom](#)

Cross Site Script Vulnerability on module "Content" in NavigateCMS 2.9 #12

🔒 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 "Content" 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 "Content"
4. Chose:
 - Go to "/navigate/navigate.php?fid=blocks"
 - Go to "/navigate/navigate.php?fid=files"
 - Go to "/navigate/navigate.php?fid=comments"
5. Click "Create" >> Insert Payload:


```
'> <details/open/ontoggle=confirm(1337)>
```
6. Save: XSS alert Message!

/Expected behavior/

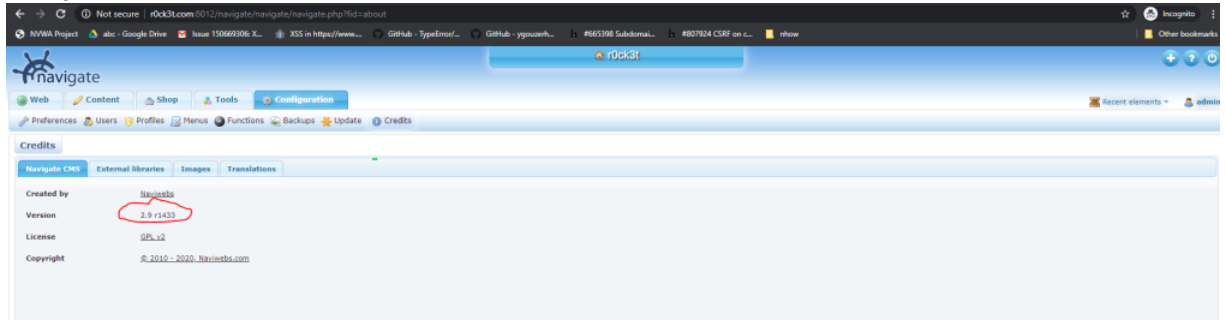
The removal of script tags is not sufficient to prevent an XSS attack. You must HTML Entity encode any output that is reflected back to the page

/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=blocks"

The screenshot shows the 'Blocks / Create' form in the rck3t.com web application. The 'Title' field is highlighted with a red circle and contains the payload: `<details/open/ontoggle=confirm(1337)>`. Below the form, a modal dialog displays the message: `www.rck3t.com:8012 says 1337`.

ID	Type	Title	Publish date	Access	Enabled	Notes
7	Slide on Homepage	Details	00 - 00			
1	Sidebar Content	Twitter widget	00 - 00			20
2	Slide on Homepage	Slide 3	00 - 00			20
3	Slide on Homepage	Slide 2	00 - 00			20
4	Slide on Homepage	Slide 1	00 - 00			20
5	Social links	Social links	00 - 00			20

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

The screenshot shows the 'Files' section of the rck3t.com web application. A modal dialog displays the message: `www.rck3t.com:8012 says rck3t`. Below the modal, the 'Files' section shows a folder named 'Theme_Kit'.

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

ID	Type	Content	Creation date	User	Text	Status
2	Element		2020-06-17 15:16			Published

/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 "Content" in NavigateCMS 2.9~~ Cross Site Script Vulnerability on module "Content" in NavigateCMS 2.9 on Jun 17, 2020

NavigateCMS commented on Jun 18, 2020

Owner

Fixed by 05873cf

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

