New issue

Jump to bottom

Cross Site Script Vulnerability on module "Configuration" in NavigateCMS 2.9 #11

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 "Configuration" feature Navigate

/To Reproduce/
Steps to reproduce the behavior:

1. Login into the panel
2. Go to '/navigate/navigate.php?fid=about'
3. Go to Moudle "Configuration"
4. Chose:

- Go to "/navigate/navigate.php?fid=users"
- Go to "/navigate/navigate.php?fid=profiles"
- Go to "/navigate/navigate.php?fid=menus"
- Go to "/navigate/navigate.php?fid=functions"
- Go to "/navigate/navigate.php?fid=backups"

5. Click "Create" >> Insert Payload:

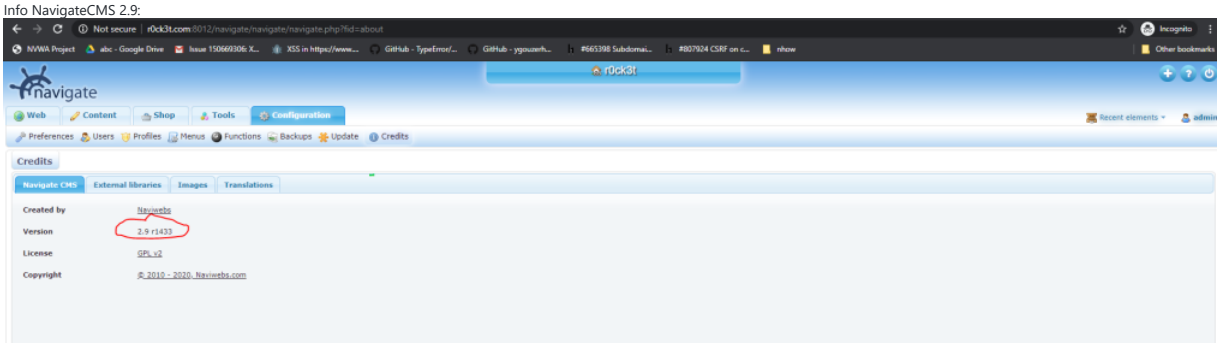
'><details/open/ontoggle=confirm(1337)>

6. Save: XSS alert Message!

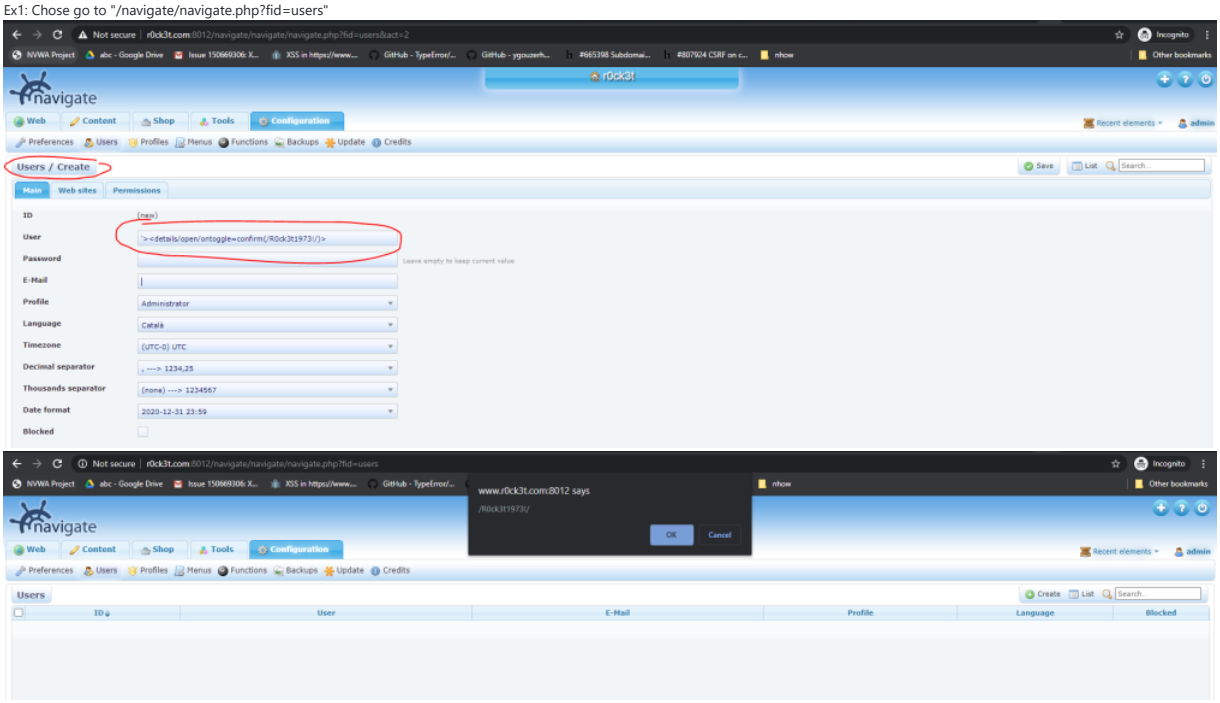
/Expected behavior/
The removal of script tags is not sufficient to prevent an XSS attack. You must HTML Entity encode any output that is reflected back to the page

/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.

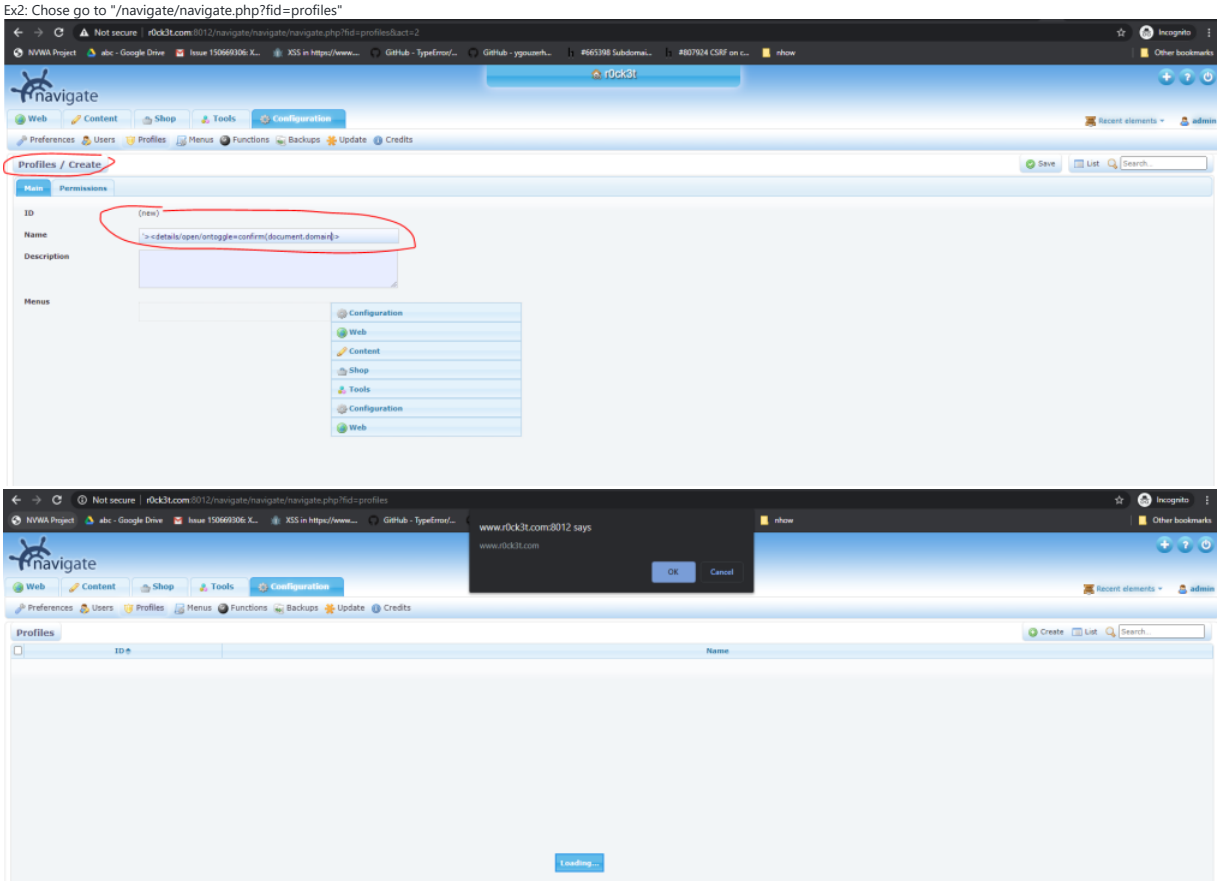
/Screenshots/
Info NavigateCMS 2.9:



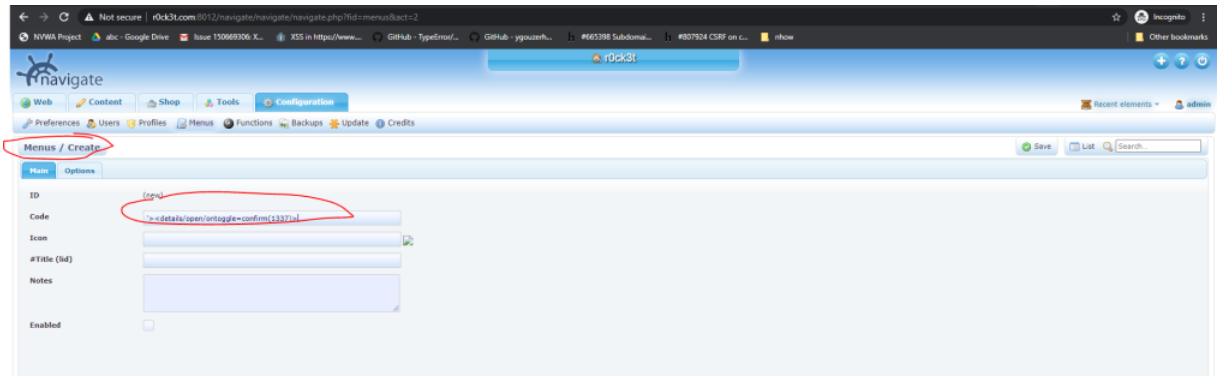
Ex1: Chose go to "/navigate/navigate.php?fid=users"

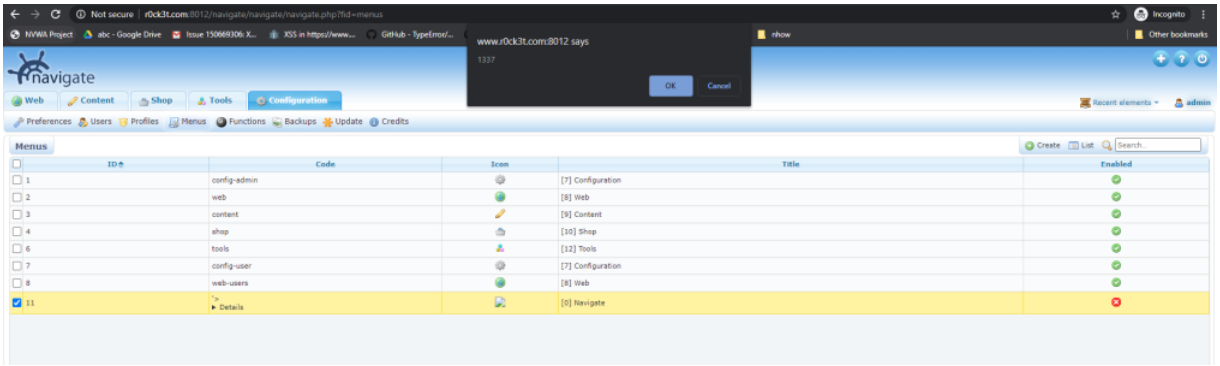


Ex2: Chose go to "/navigate/navigate.php?fid=profiles"

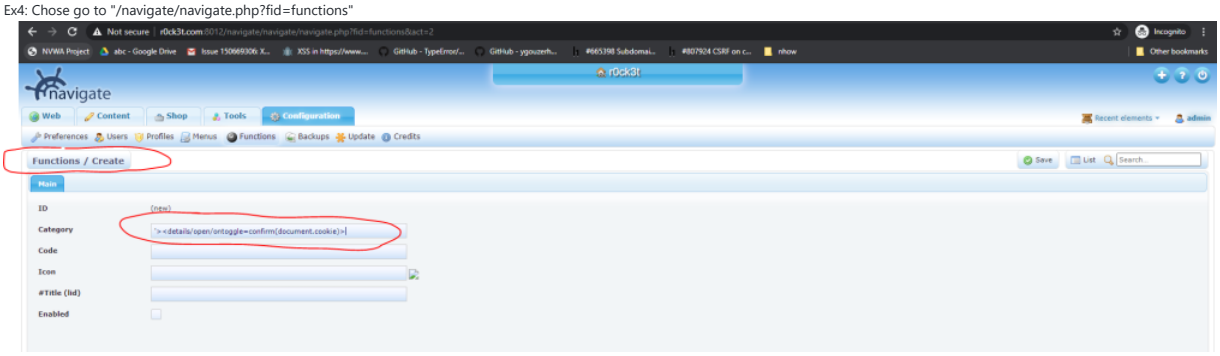


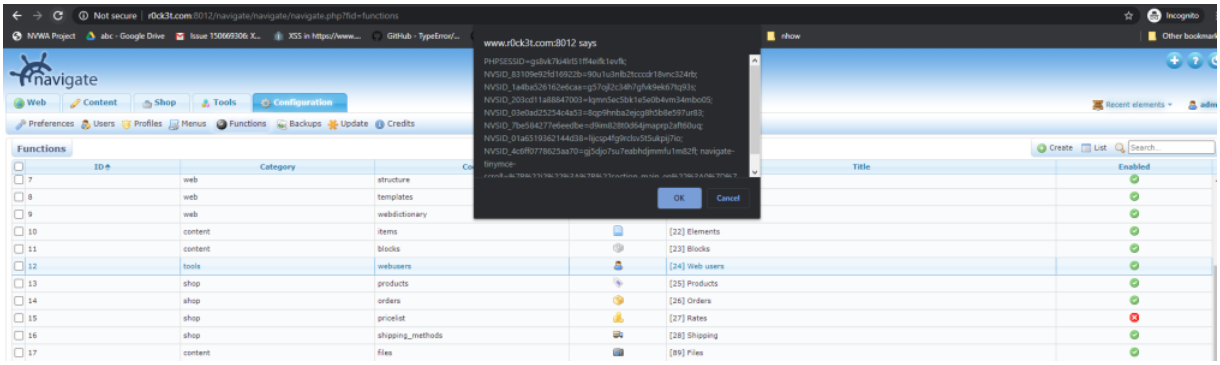
Ex3: Chose go to "/navigate/navigate.php?fid=menus"



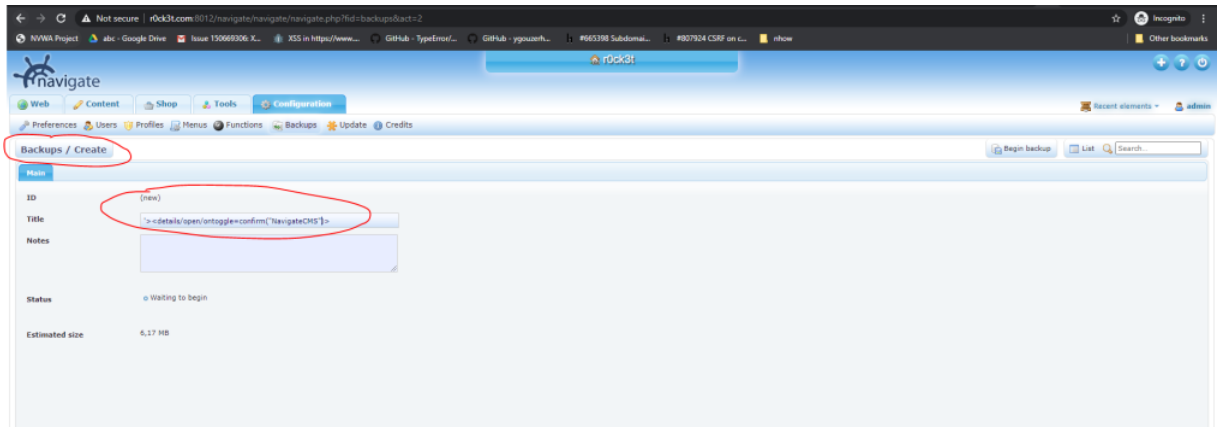


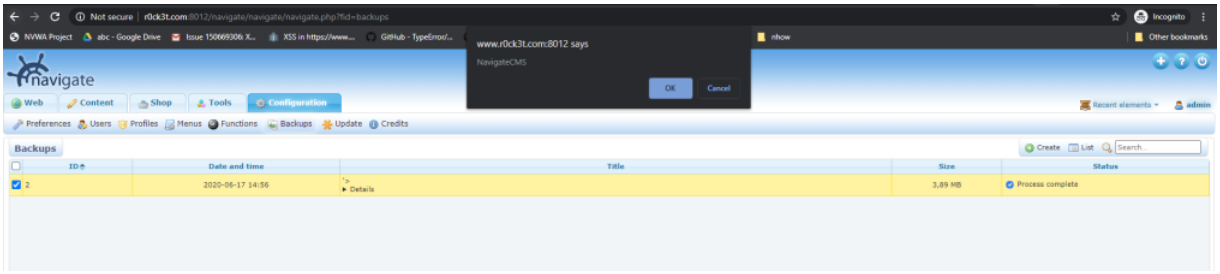
Ex4: Chose go to "/navigate/navigate.php?fid=functions"





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





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

NavigateCMS commented on Jun 18, 2020 — Owner

Fixed by `ed8ba30`

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 assigne!

Thanks you!

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants