New issue

Jump to bottom

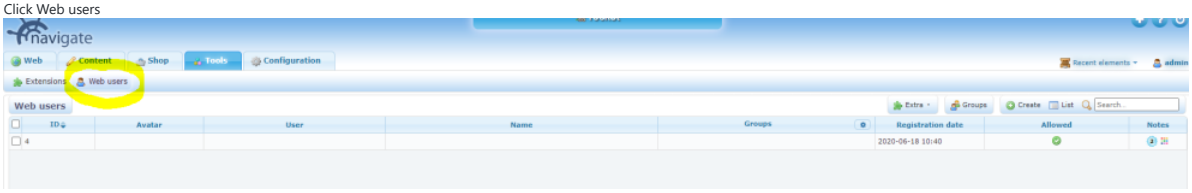
Cross Site Script Vulnerability on "Tools" feature in NavigateCMS 2.9 #16

Closed **luuthehienhbit** opened this issue on Jun 18, 2020 · 2 comments

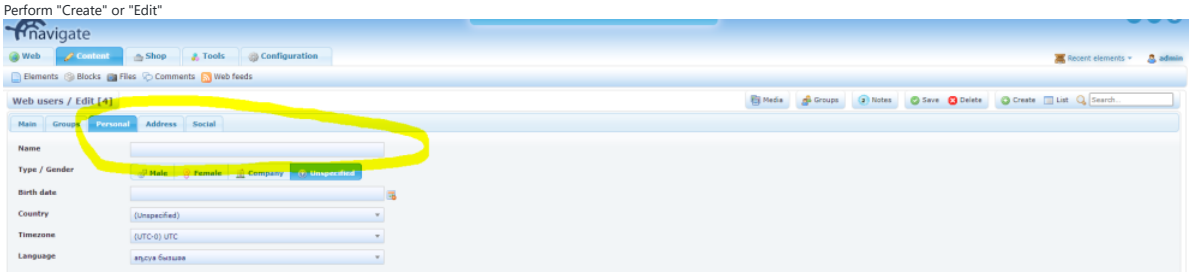
luuthehienhbit commented on Jun 18, 2020

Expected behaviour
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Tools" feature.
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.
Steps to reproduce

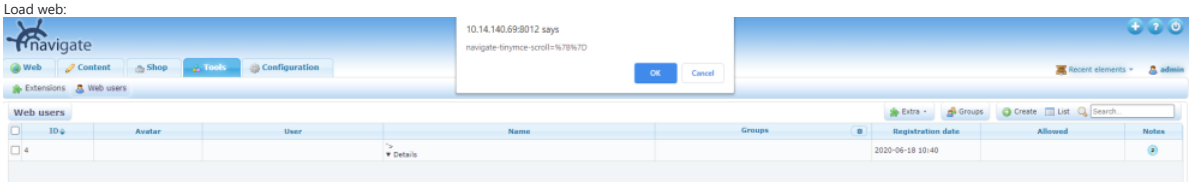
1. Log into the Admin.
2. Go to function "Tools"
3. Click Web users



4. Perform "Create" or "Edit"



5. Add payload in name via Personal: '><details/open/ontoggle=confirm(document.cookie)>
6. Load web:



NavigateCMS 2.9

NavigateCMS commented on Jun 18, 2020 Owner

Fixed by `68e1870`

NavigateCMS closed this as completed on Jun 18, 2020

r0ck3t1973 commented on Jun 18, 2020

Hi Team Security **@NavigateCMS**

You can a CVE ID assigne!

Thanks you!

2

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants