New issue

Jump to bottom

Cross Site Script Vulnerability on "connections" in WebPort-v1.19.17121 #1

Closed **r0ck3t1973** opened this issue on Jun 22, 2020 · 0 comments

r0ck3t1973 commented on Jun 22, 2020 Owner

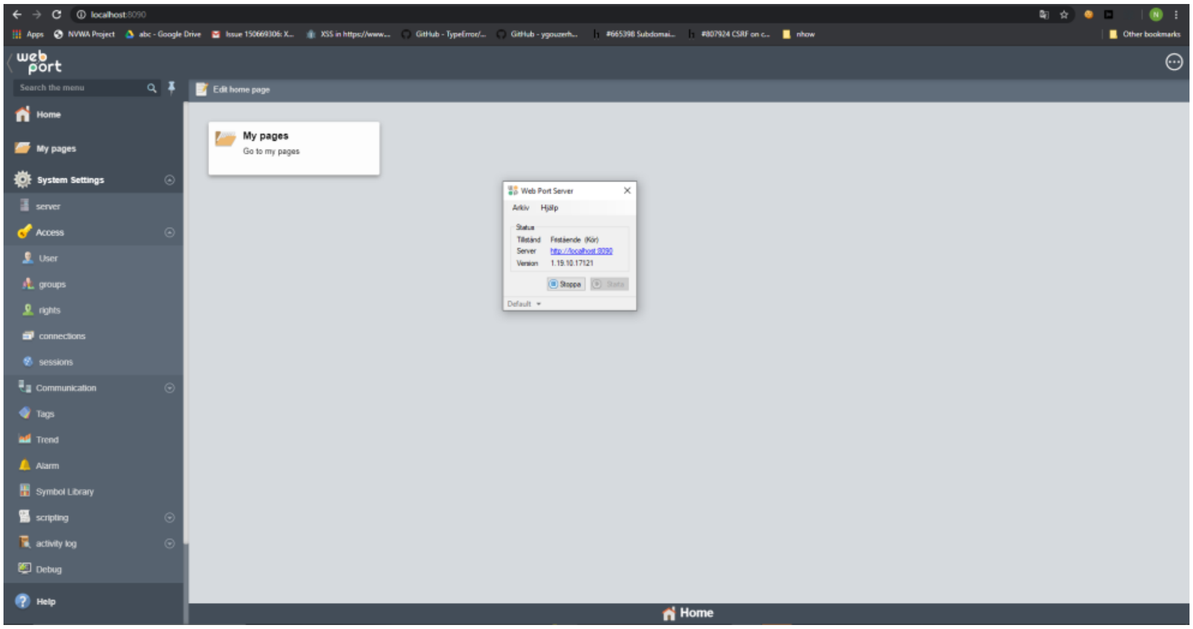
Describe the bug
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "connections" feature.

To Reproduce
Steps to reproduce the behavior:

1, Login into the panel
2. Go to '/access/setup?type=conn'
3. Change connections
4. Insert Payload:
'><details/open/ontoggle=confirm(1337)>
5. 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

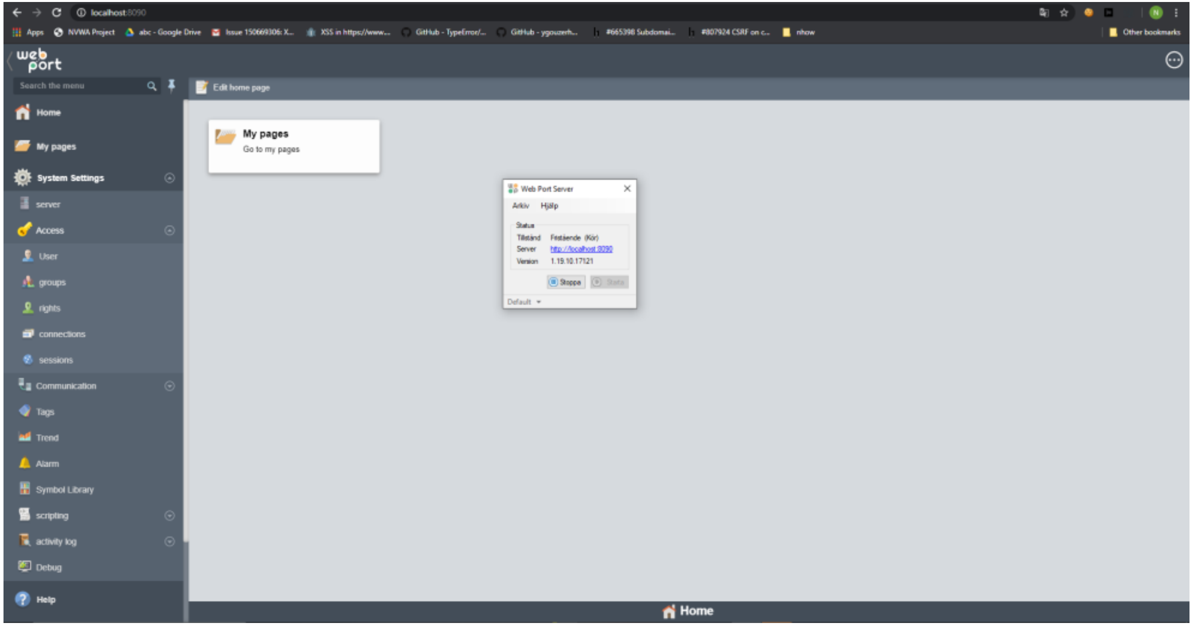
Screenshots

1. Info WebPort-v1.19.17121



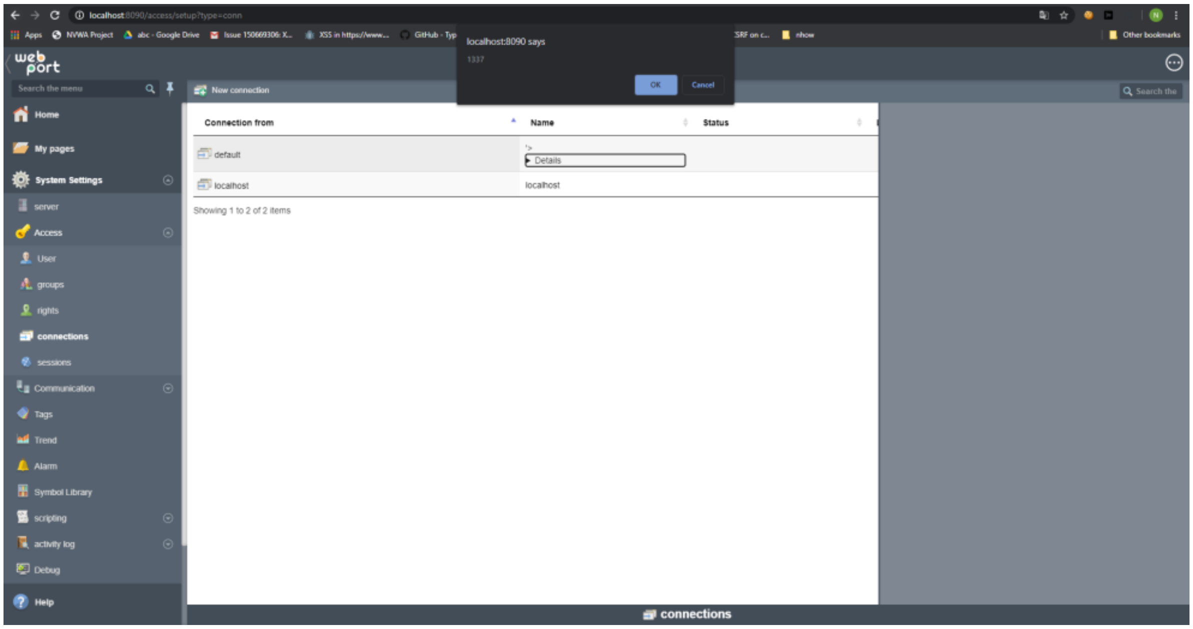
Status
Tillstånd Fristående (Kör)
Server http://localhost:8090
Version 1.19.10.17121

2. Insert payload



Status
Tillstånd Fristående (Kör)
Server http://localhost:8090
Version 1.19.10.17121

3. xss alert mess



localhost:8090 says

1337

Connection from	Name	Status
default	'> ▶ Details	
localhost	localhost	

Showing 1 to 2 of 2 items

Desktop (please complete the following information):

OS: Windows
Browser Chorme
Version: Version 83.0.4103.106

r0ck3t1973 closed this as completed on Sep 1, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant