New issue

Jump to bottom

Cross Site Script Vulnerability on "Configure Attributes" feature in phplist version 3.5.3 #664

Closed r0ck3t1973 opened this issue on May 25, 2020 · 1 comment

r0ck3t1973 commented on May 25, 2020

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

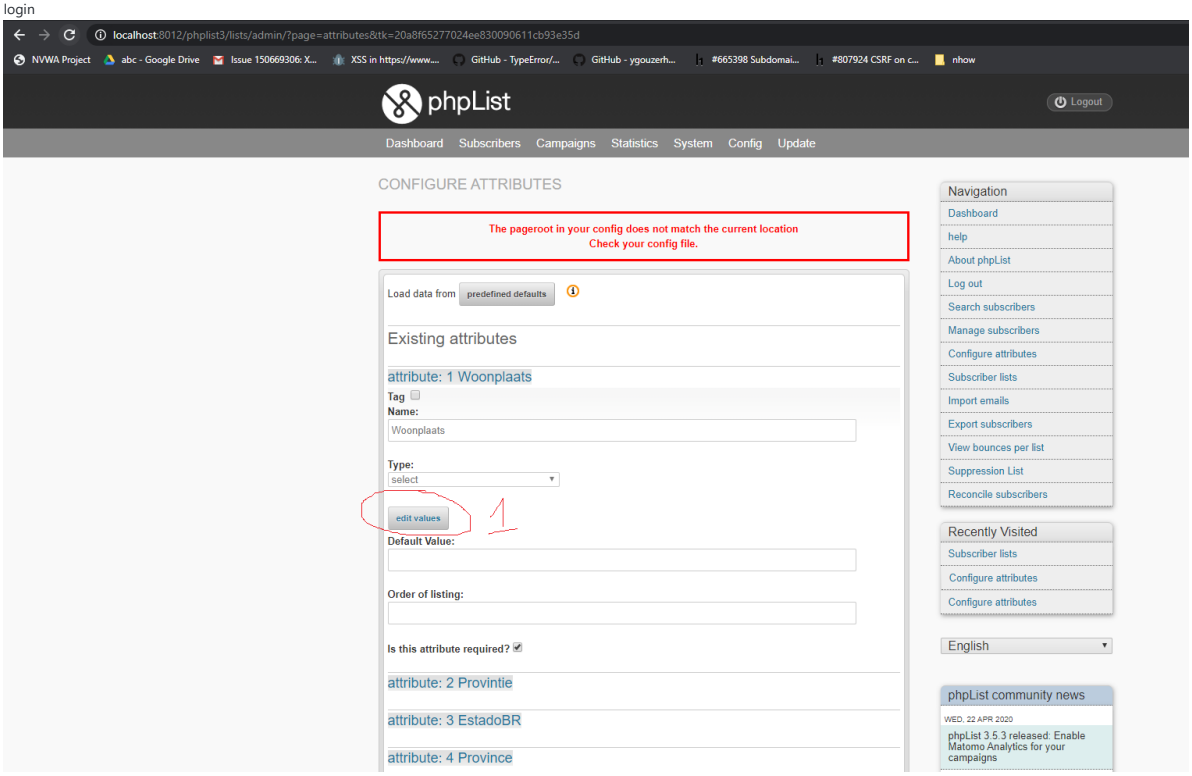
To Reproduce
Steps to reproduce the behavior:

1. Login into the panel phplist
2. Go to 'phplist3/lists/admin/?page=attributes&tk=20a8f65277024ee830090611cb93e35d'
3. Click 'Edit Values' -> 'Add new'
4. Insert Payload XSS:
   '><details/open/ontoggle=confirm(1337)>
5. Add new Woonplaats
6. xss alert message

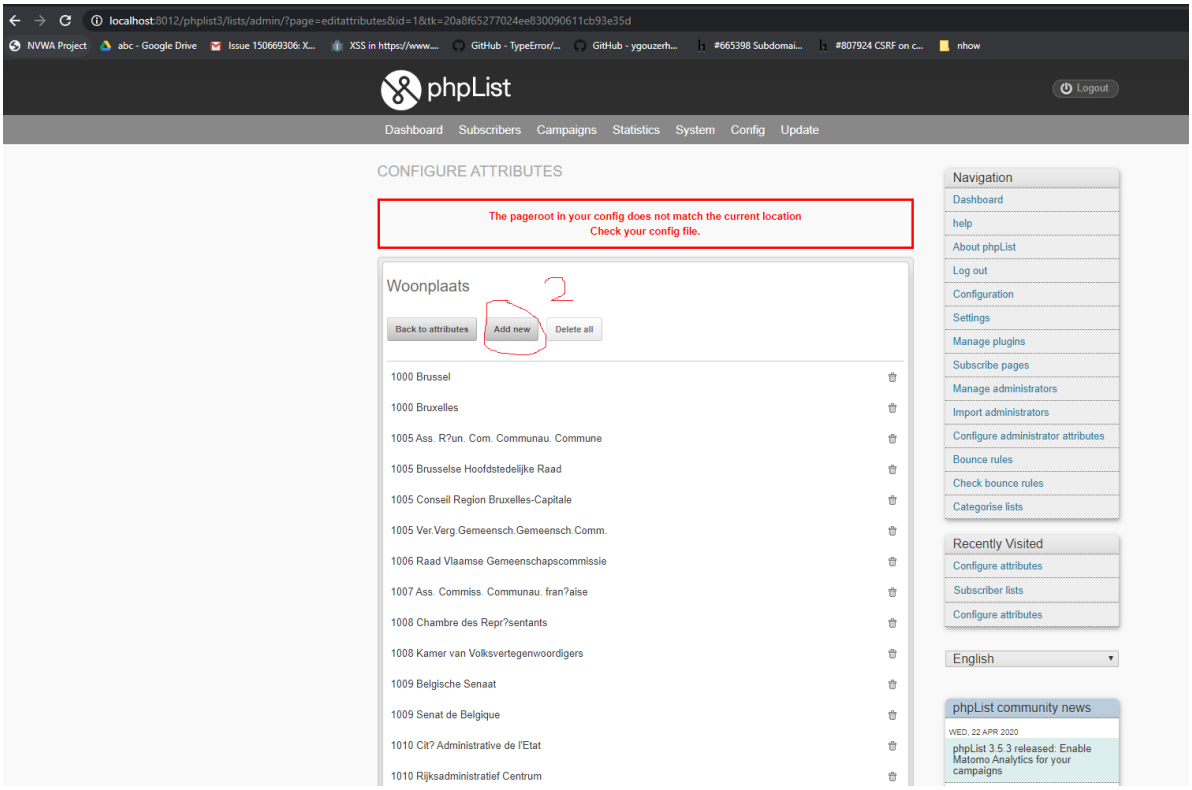
Expected behavior
The removal of script tags is not sufficient to prevent an XSS attack. You must HTML Entity encode any output that is reflected back to the page

Screenhost

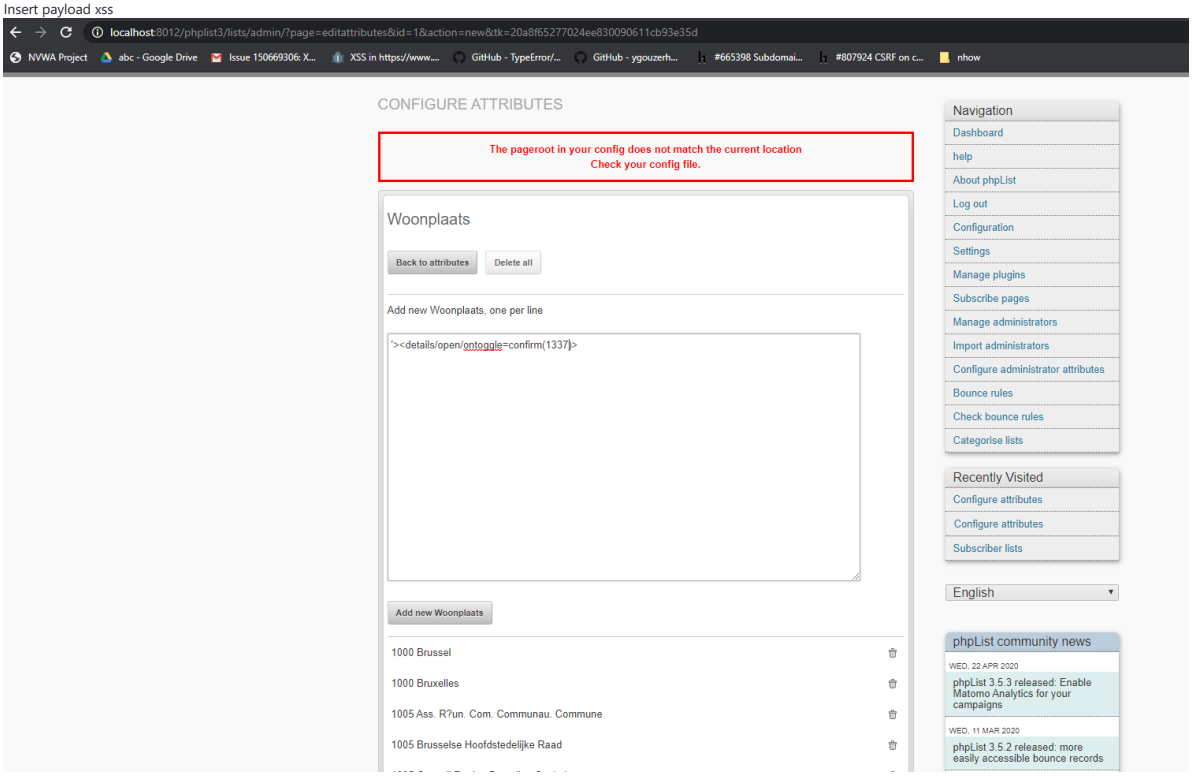
1. login



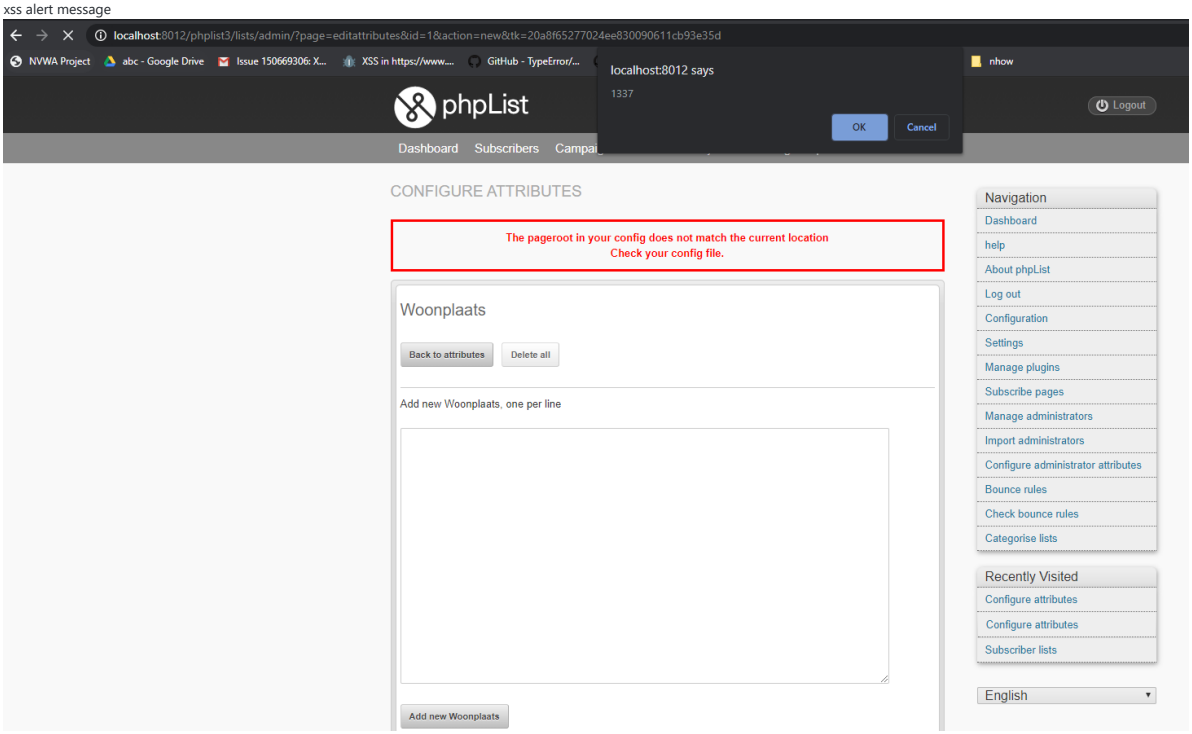
2. Add new



3. Insert payload xss



4. xss alert message



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

I Hope you fix it ASAP

michield commented on May 26, 2020 — Member

fixed in `e222600`

michield closed this as completed on May 26, 2020

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants