

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:

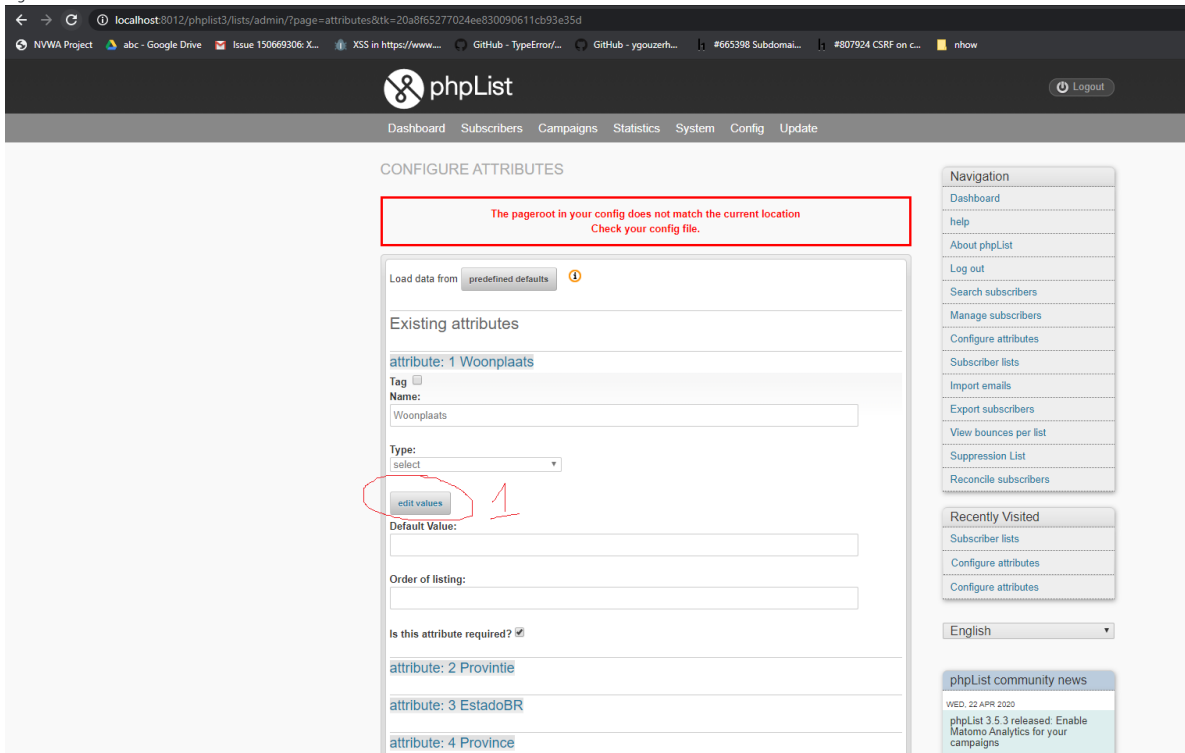
1. Login into the panel phplist
2. Go to 'phplist3/lists/admin/?page=attributes&tk=20a8f65277024ee830090611cb93e35d'
3. Click 'Edit Values' -> 'Add new'
4. Insert Payload XSS:
'><details/open/ontoggle=confirm(1337)>
5. Add new Woonplaats
6. xss alert message

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

localhost:8012/phplist3/lists/admin/?page=editattributes&id=1&tk=20a8f65277024ee830090611cb93e35d

NVWA Project abc - Google Drive Issue 150669306: XSS in https://www... GitHub - TypeError/... GitHub - ygouzerh... #665398 Subdomai... #807924 CSRF on c... nhow

phpList Logout

Dashboard Subscribers Campaigns Statistics System Config Update

CONFIGURE ATTRIBUTES

The pageroot in your config does not match the current location
Check your config file.

Woonplaats

Back to attributes Add new Delete all

1000 Brussel	
1000 Bruxelles	
1005 Ass. R?un. Com. Communau. Commune	
1005 Brusselse Hoofdstedelijke Raad	
1005 Conseil Region Bruxelles-Capitale	
1005 Ver.Verg. Gemeensch. Gemeensch. Comm.	
1006 Raad Vlaamse Gemeenschapscommissie	
1007 Ass. Commiss. Communau. fran?aise	
1008 Chambre des Repr?sentants	
1008 Kamer van Volksvertegenwoordigers	
1009 Belgische Senaat	
1009 Senat de Belgique	
1010 Cir? Administrative de l'Etat	
1010 Rijksadministratief Centrum	

Navigation

- Dashboard
- help
- About phpList
- Log out
- Configuration
- Settings
- Manage plugins
- Subscribe pages
- Manage administrators
- Import administrators
- Configure administrator attributes
- Bounce rules
- Check bounce rules
- Categorise lists

Recently Visited

- Configure attributes
- Subscriber lists
- Configure attributes

English

phpList community news

WED. 22 APR 2020

phpList 3.5.3 released: Enable Matomo Analytics for your campaigns

3. Insert payload xss

localhost:8012/phplist3/lists/admin/?page=editattributes&id=1&action=new&tk=20a8f65277024ee830090611cb93e35d

NVWA Project abc - Google Drive Issue 150669306: XSS in https://www... GitHub - TypeError/... GitHub - ygouzerh... #665398 Subdomai... #807924 CSRF on c... nhow

phpList Logout

Dashboard Subscribers Campaigns Statistics System Config Update

CONFIGURE ATTRIBUTES

The pageroot in your config does not match the current location
Check your config file.

Woonplaats

Back to attributes Delete all

Add new Woonplaats, one per line

><details/open?ontop&is=confirm(1337)>

Add new Woonplaats

1000 Brussel	
1000 Bruxelles	
1005 Ass. R?un. Com. Communau. Commune	
1005 Brusselse Hoofdstedelijke Raad	

Navigation

- Dashboard
- help
- About phpList
- Log out
- Configuration
- Settings
- Manage plugins
- Subscribe pages
- Manage administrators
- Import administrators
- Configure administrator attributes
- Bounce rules
- Check bounce rules
- Categorise lists

Recently Visited

- Configure attributes
- Configure attributes
- Subscriber lists

English

phpList community news

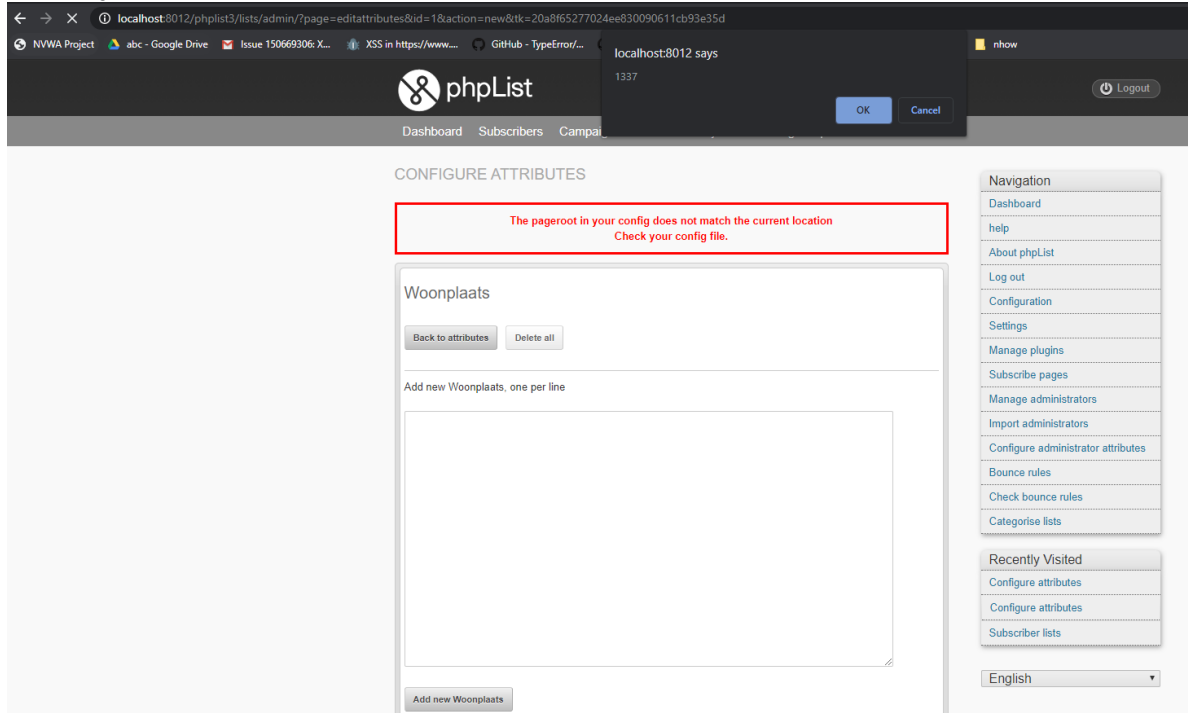
WED. 22 APR 2020

phpList 3.5.3 released: Enable Matomo Analytics for your campaigns

WED. 11 MAR 2020

phpList 3.5.2 released: more easily accessible bounce records

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

