New issue

Jump to bottom

Cross Site Script Vulnerability on "Categories Lists" feature in phplist version 3.5.3 #669

Closed r0ck3t1973 opened this issue on May 27, 2020 · 3 comments

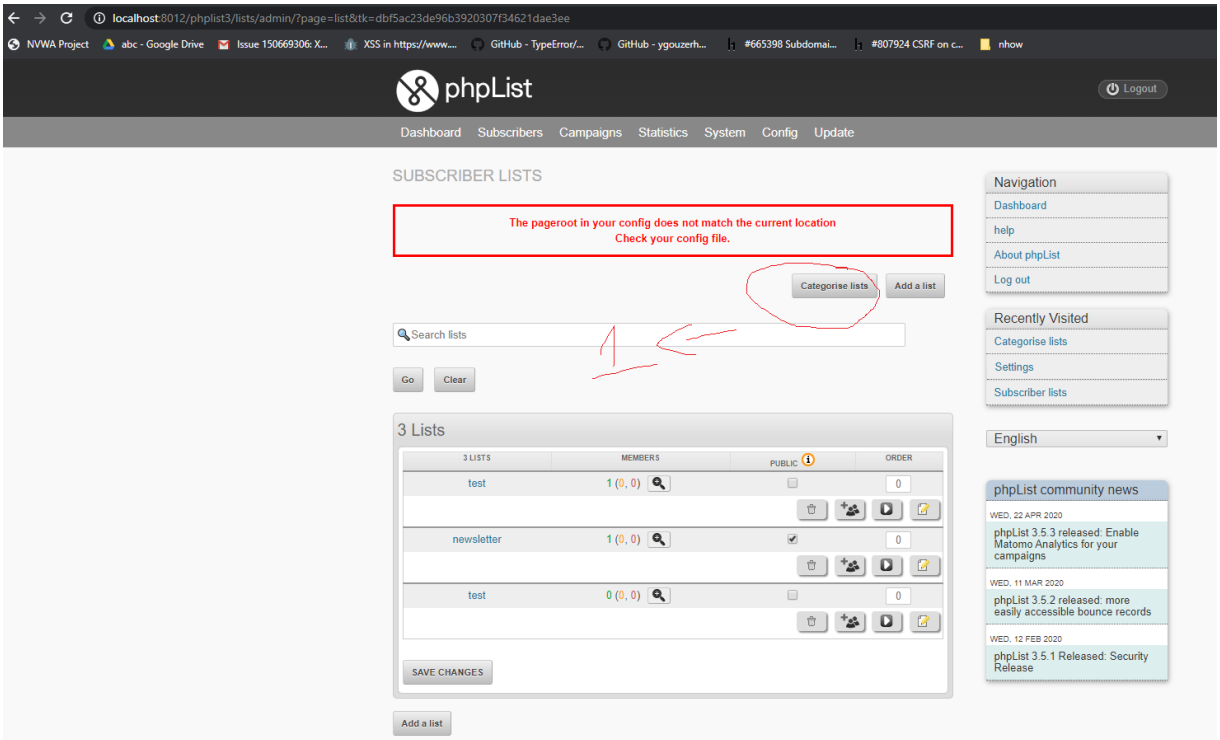
r0ck3t1973 commented on May 27, 2020

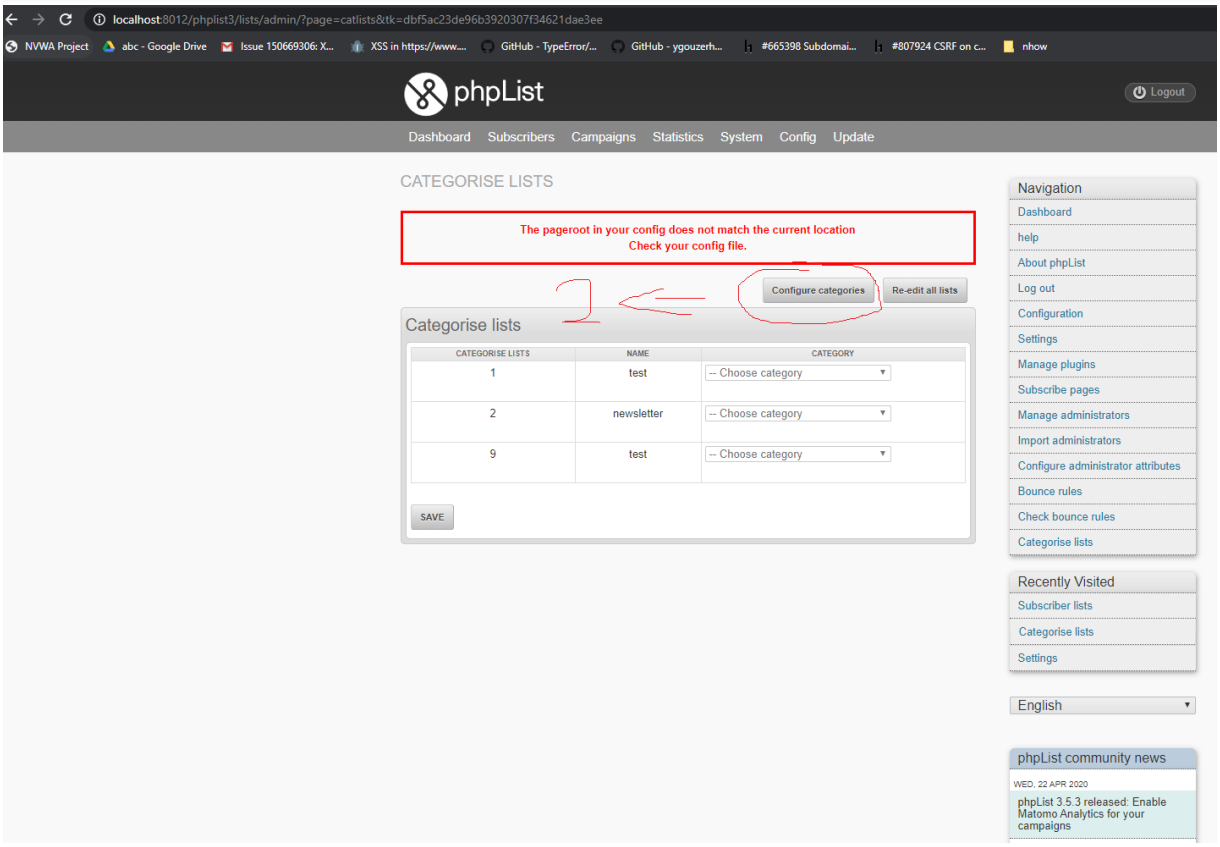
Describe the bug
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Categories Lists" feature.

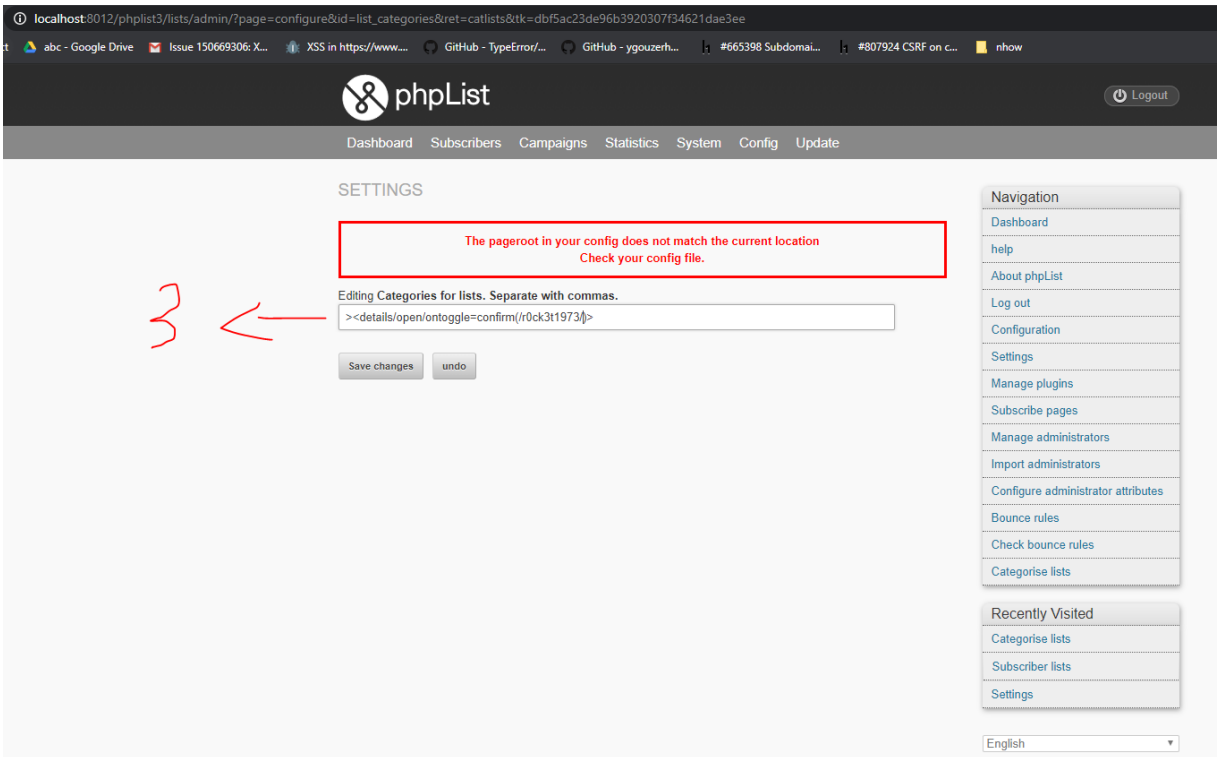
To Reproduce
Steps to reproduce the behavior:

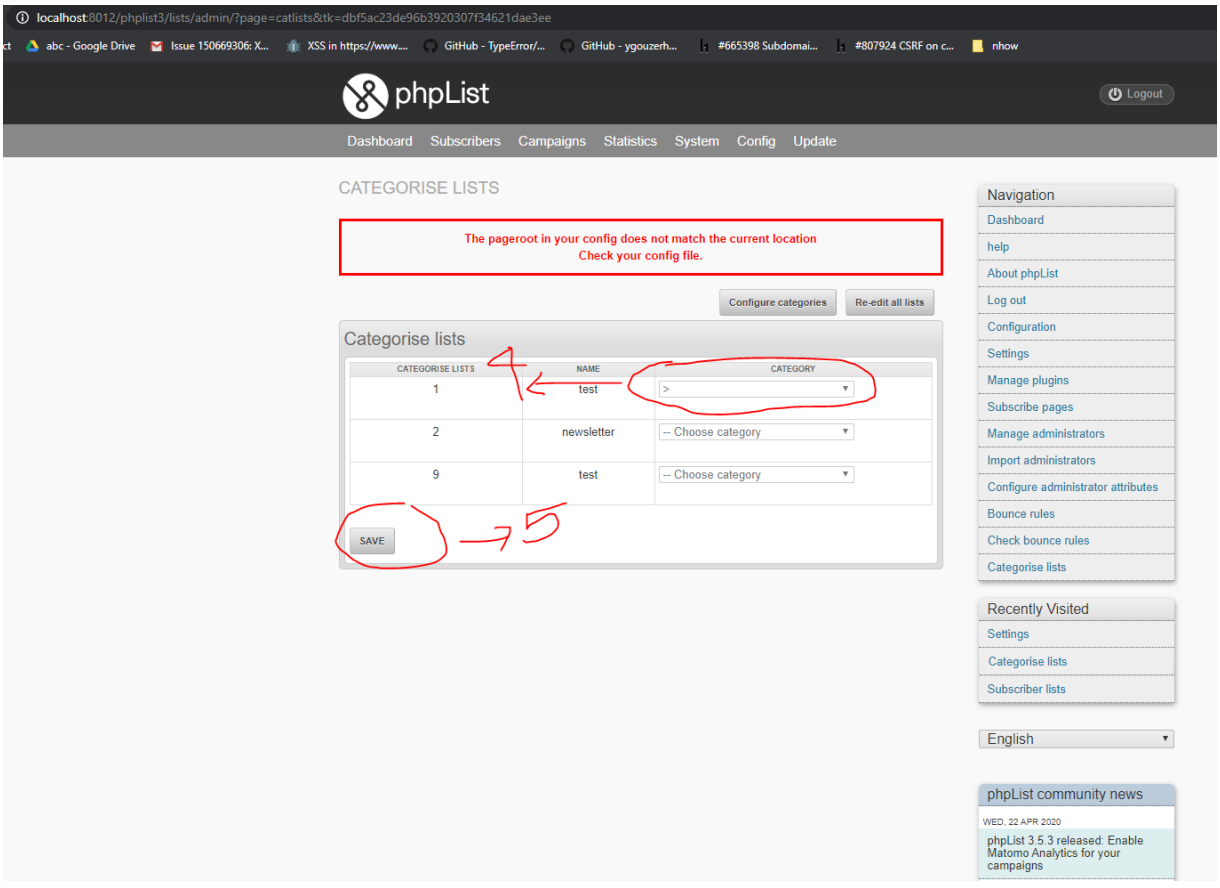
1. Login into the panel phplist
2. Go to 'phplist3/lists/admin/?page=list&tk=dbf5ac23de96b3920307f34621dae3ee'
3. Click 'Subscribers Lists' -> 'Categories Lists' -> 'Configure Categories'
4. Insert Payload XSS:
   '><details/open/ontoggle=confirm(/r0ck3t1973/)>
5. Save and Back -> click chose 'CATEGORY' new -> Save -> click Subscribers
6. xss alert message

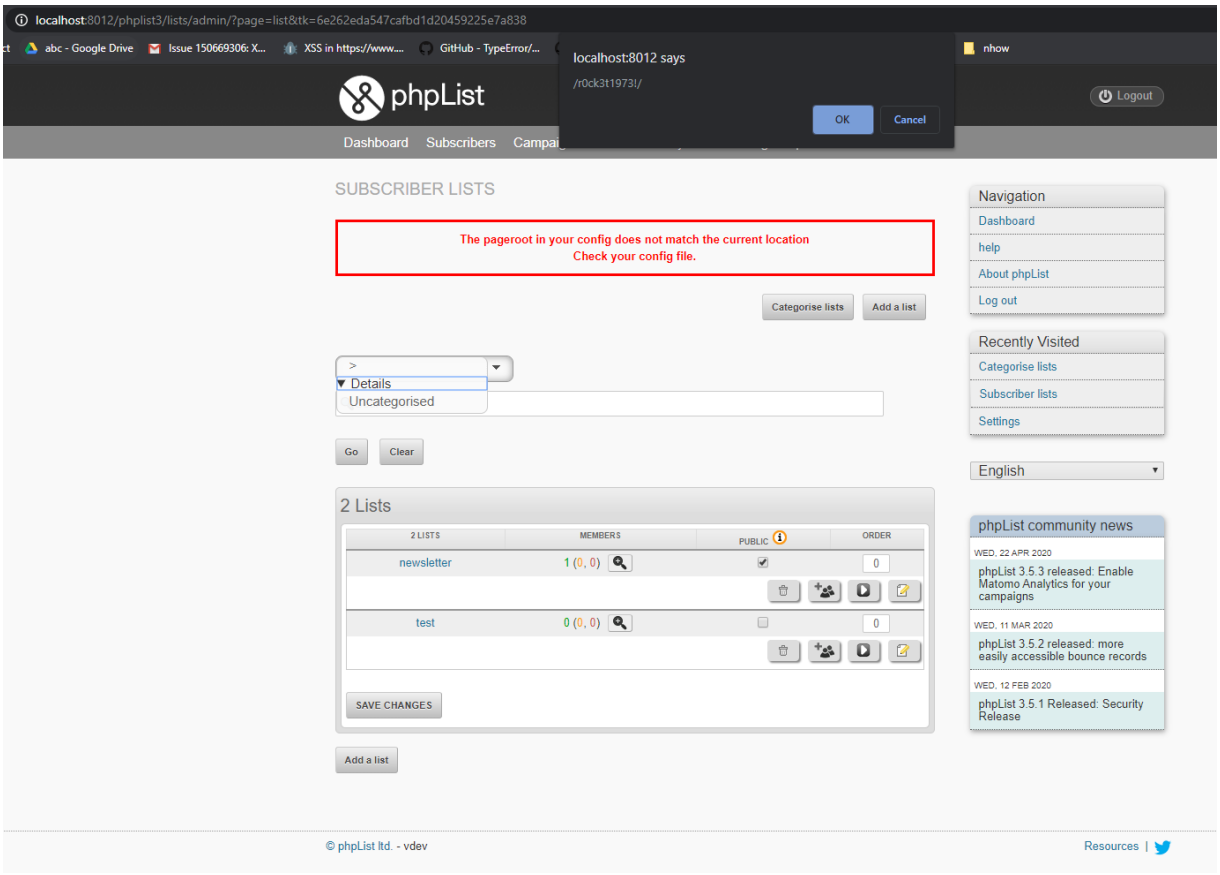
Screenhost


localhost:8012/phplist3/lists/admin/?page=list&tk=dbf5ac23de96b3920307f34621dae3ee
phpList
Logout
Dashboard Subscribers Campaigns Statistics System Config Update
SUBSCRIBER LISTS
The pageroot in your config does not match the current location
Check your config file.
Categorise lists
Add a list
Search lists
Go
Clear
3 Lists
3 LISTS
MEMBERS
PUBLIC
ORDER
test
1 (0, 0)
newsletter
1 (0, 0)
test
0 (0, 0)
SAVE CHANGES
Add a list
Navigation
Dashboard
help
About phpList
Log out
Recently Visited
Categorise lists
Settings
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
WED, 12 FEB 2020
phpList 3.5.1 Released: Security Release
© phpList ltd. - vdev
Resources


localhost:8012/phplist3/lists/admin/?page=catlists&tk=dbf5ac23de96b3920307f34621dae3ee
phpList
Logout
Dashboard Subscribers Campaigns Statistics System Config Update
CATEGORISE LISTS
The pageroot in your config does not match the current location
Check your config file.
Configure categories
Re-edit all lists
Categorise lists
CATEGORISE LISTS
NAME
CATEGORY
1
test
-- Choose category
2
newsletter
-- Choose category
9
test
-- Choose category
SAVE
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
Subscriber lists
Categorise lists
Settings
English
phpList community news
WED, 22 APR 2020
phpList 3.5.3 released: Enable Matomo Analytics for your campaigns


localhost:8012/phplist3/lists/admin/?page=configure&id=list_categories&ret=catlists&tk=dbf5ac23de96b3920307f34621dae3ee
phpList
Logout
Dashboard Subscribers Campaigns Statistics System Config Update
SETTINGS
The pageroot in your config does not match the current location
Check your config file.
Editing Categories for lists. Separate with commas.
><details/open/ontoggle=confirm(/r0ck3t1973/)>
Save changes
undo
3
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
Categorise lists
Subscriber lists
Settings
English


localhost:8012/phplist3/lists/admin/?page=catlists&tk=dbf5ac23de96b3920307f34621dae3ee
phpList
Logout
Dashboard Subscribers Campaigns Statistics System Config Update
CATEGORISE LISTS
The pageroot in your config does not match the current location
Check your config file.
Configure categories
Re-edit all lists
Categorise lists
CATEGORISE LISTS
NAME
CATEGORY
1
test
>
2
newsletter
-- Choose category
9
test
-- Choose category
SAVE
4
5
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
Settings
Categorise lists
Subscriber lists
English
phpList community news
WED, 22 APR 2020
phpList 3.5.3 released: Enable Matomo Analytics for your campaigns



Also Video PoC
https://drive.google.com/open?id=1ZY7QpWzg9SEkjXQsBCRUs-up8U0Yh1L2

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.

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

I Hope you fix it ASAP!!!

michield commented on May 27, 2020 — Member

Fixed with `ba8507f`

michield closed this as completed on May 27, 2020

suelaP commented on May 29, 2020 — Member

@r0ck3t1973 thank you for your contributions again :). The fixes to all issues you reported have been included in the latest release. You can take a look at the release notes here:
https://www.phplist.org/newslist/phplist-3-5-4-release-notes/

r0ck3t1973 commented on May 29, 2020 — Author

Hi Team Security phplist3.

You can a CVE ID assigned and reference change log to "UraSec Team" :D

Thanks you!
...

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants