

New issue

[Jump to bottom](#)

Cross Site Script Vulnerability on "Subscribers Lists" feature in phplist version 3.5.3 #666

🔒 Closed r0ck3t1973 opened this issue on May 25, 2020 · 4 comments

r0ck3t1973 commented on May 25, 2020 • edited

Describe the bug

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

To Reproduce

Steps to reproduce the behavior:


1. Login into the panel phplist
2. Go to 'phplist3/lists/admin/?page=list&tk=5346bb7f96da80c4ac675b4fe5b21f60'
3. Click 'Subscribers Lists' -> 'Add a lists'
4. Insert Payload XSS: 'to email address(es)'
'><details/open/ontoggle=confirm(1337)>
5. Save -> Click 'Config' -> 'Add some subscribers'
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

localhost:8012/phpList3/lists/admin/?page=list&tk=3a541ab512968bc0b42436daec9487c1

NVWA Project abc - Google Drive Issue 150669306: XSS in https://www... GitHub - TypeError... GitHub - ygouzerh... #663398 Subdomai... #807924 CSRF on c... rhov

 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](#)

[Go](#) [Clear](#)

2 Lists

2 LISTS	MEMBERS	PUBLIC	ORDER
test	1 (0, 0)	<input type="checkbox"/>	0
newsletter	1 (0, 0)	<input checked="" type="checkbox"/>	0

[SAVE CHANGES](#)

[Add a list](#)

[Navigation](#)
[Dashboard](#)
[help](#)
[About phpList](#)
[Log out](#)

[Recently Visited](#)
[Edit a list](#)
[Subscriber lists](#)
[Import subscribers by copy-and-paste](#)


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](#) | [Twitter](#)

localhost:8012/phpList3/lists/admin/?page=editlist&tk=5346bb7f96da80c4ac675b4fe5b21f60

NVWA Project abc - Google Drive Issue 150669306: XSS in https://www... GitHub - TypeError... GitHub - ygouzerh... #663398 Subdomai... #807924 CSRF on c... rhov

 phpList [Logout](#)

[Dashboard](#) [Subscribers](#) [Campaigns](#) [Statistics](#) [System](#) [Config](#) [Update](#)

EDIT A LIST

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

☐
Public list (listed on the frontend)
Order for listing
0

List Description
><details/open/ontoggle=confirm(1337)></div>

[Save](#) [Cancel](#)

[Navigation](#)
[Dashboard](#)
[help](#)
[About phpList](#)
[Log out](#)

[Recently Visited](#)
[Subscriber lists](#)
[Configuration](#)
[Import subscribers by copy-and-paste](#)

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](#) | [Twitter](#)

localhost:8012/phplist3/lists/admin/?page=setup&tk=5346bb7f96da80c4ac675b4fe5b21f60

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

phpList

Dashboard Subscribers Campaigns Statistics System Config Update

CONFIGURATION

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

Configuration steps

Step	Status
Initialise Database	✓
Verify settings	✓
Configure attributes	✓
Create public lists	✓
Create a subscribe page	✓
Add some subscribers	✗

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

- Edit a list
- Subscriber lists
- Configuration

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=import&tk=5346bb7f96da80c4ac675b4fe5b21f60

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

phpList

Dashboard Subscribers Campaigns Statistics System Config Update

IMPORT EMAILS

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

Please choose one of the import methods below

copy and paste list of emails

import by uploading a file with emails

import by uploading a CSV file with emails and additional data

Navigation

- Dashboard
- help
- About phpList
- Log out
- Search subscribers
- Manage subscribers
- Configure attributes
- Subscriber lists
- Import emails
- Export subscribers
- View bounces per list
- Suppression List
- Reconcile subscribers

Recently Visited

- Configuration
- Edit a list
- Subscriber lists

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=importsimple&tk=5346bb7f96da80c4ac675b4fe5b21f60

NVWA Projectabc - Google DriveIssue 150669306: XSS in https://www...GitHub - TypeError...localhost8012 says1337

phpList

localhost8012 says1337

OKCancel

Logout

DashboardSubscribersCampai

IMPORT SUBSCRIBERS BY COPY-AND-PASTE

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

Select the lists to add the emails to

☐ All Lists

☐ All Public Lists

☐ Demo Private list

>

Details

☐ newsletter Public list
Sign up to our newsletter

☐ test Private list
List for testing

Please enter the email addresses to import, one per line, in the box below and click "Import Emails"

Navigation

Dashboard

help

About phpList

Log out

Search subscribers

Manage subscribers

Configure attributes

Subscriber lists

Import emails

Export subscribers

View bounces per list

Suppression List

Reconcile subscribers

Recently Visited

Import emails

Configuration

Edit a list

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=1Oh0-YcP2Kombmgh2USyivptZNe-ywCa4>

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!!!

Michiel commented on May 26, 2020

Member

Fixed in 9c4515c

Michiel closed this as completed on May 26, 2020

r0ck3t1973 commented on May 26, 2020

Author

Hi @Michiel, I found a small bug "Subscribers Lists"!

Screenhost:

The screenshot shows the phpList 3.5.3 admin interface. At the top, a dark header bar contains the phpList logo, navigation links (Dashboard, Subscribers, Campaigns), and a user profile for 'nhov' with a 'Logout' button. A modal window is open, displaying the message: 'localhost:8012 says /r0ck3t1973/'. Below the header, the main content area is titled 'SUBSCRIBER LISTS'. A red-bordered box highlights an error message: 'The pageroot in your config does not match the current location. Check your config file.' To the right of the main content is a sidebar with 'Navigation' links (Dashboard, help, About phpList, Log out), 'Recently Visited' links (Categorise lists, Subscriber lists, Settings), and a language selector set to 'English'. Below the sidebar is a 'phpList community news' section with three items dated from February to April 2020. The main content area features a search bar with a dropdown menu showing 'Details' and 'Uncategorised'. Below the search bar is a table titled '2 Lists' with columns for '2 LISTS', 'MEMBERS', 'PUBLIC', and 'ORDER'. The table contains two rows: 'newsletter' with 1 member and 'test' with 0 members. At the bottom of the table is a 'SAVE CHANGES' button. A footer bar at the very bottom contains '© phpList Ltd. - vdev' and 'Resources | Twitter'.

Also Video PoC:

<https://drive.google.com/open?id=1ZY7QpWzg9SEkXQs8CRUs-up8U0Yh1L2>

suelaP commented on May 27, 2020

Member

@r0ck3t1973 thank you for your reports :) This looks like a separate issue related to List categories. Would you mind creating a new one for this report?

r0ck3t1973 commented on May 27, 2020

Author

@suelaP Ok!
Tkanks,

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

