

New issue

Jump to bottom

# Bypass Cross Site Scripting Vulnerability on "IMPORT EMAILS" feature in php-list-3.5.4 #672

Closed r0ck3t1973 opened this issue on May 30, 2020 · 8 comments

r0ck3t1973 commented on May 30, 2020

Hi Team phplist3, I found a small bug!  
\*\*Describe the bug  
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "IMPORT EMAILS" feature. It affects both options SEND A CAMPAIGN feature.


**To Reproduce**

Steps to reproduce the behavior:

1. Login into the panel phplist
2. Go to 'phplist3/lists/admin/?page=setup&tk=1c63b88932115188325586eab8221123'
3. Chose 'Config' -> Click 'Add some subscribers' -> Chose 1/3 options (Copy and paste list of emails) -> 'Add a list'
4. Insert Payload XSS:  
X  
`<a href="j&Tab;a&Tab;v&Tab;asc&NewLine;ri&Tab;pt&colon;&lpar;a&Tab;l&Tab;e&Tab;r&Tab;t&Tab;(/by r0ck3t1973/)&rpar;">X</a>`
5. Save
6. xss alert message

localhost:8012/phpList3/lists/admin/?page=setup&tk=1c63b88932115188325586eab8221123

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

 phpList [Logout](#)

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

### CONFIGURATION

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

#### configuration steps

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

→ 1

#### Navigation

- [Dashboard](#)
- [help](#)
- [About phpList](#)
- [Log out](#)
- [Configuration](#)
- [Settings](#)
- [Manage Plugins](#)
- [Subscribe pages](#)
- [List administrators](#)
- [Import administrators](#)
- [Configure administrator attributes](#)
- [Bounce rules](#)
- [Check bounce rules](#)
- [Categorise lists](#)

#### Recently visited

- [Subscriber lists](#)
- [Import subscribers by cut-and-paste](#)
- [Import emails](#)


#### phpList community news

THU, 28 MAY 2020

phpList 3.5.4 released: Security Release

localhost:8012/phpList3/lists/admin/?page=import&tk=1c63b88932115188325586eab8221123

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


 phpList [Logout](#)


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


### IMPORT EMAILS

The pageroot in your config does not match the current locationCheck 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

→ choose 1/3

#### Continue Configuration

#### Navigation

- [Dashboard](#)
- [help](#)
- [About phpList](#)
- [Log out](#)
- [Search subscribers](#)
- [Manage subscribers](#)
- [Configure attributes](#)
- [Subscriber lists](#)
- [Import emails](#)
- [Export subscribers](#)
- [View bounces per list](#)
- [suppressionlist](#)
- [Reconcile subscribers](#)

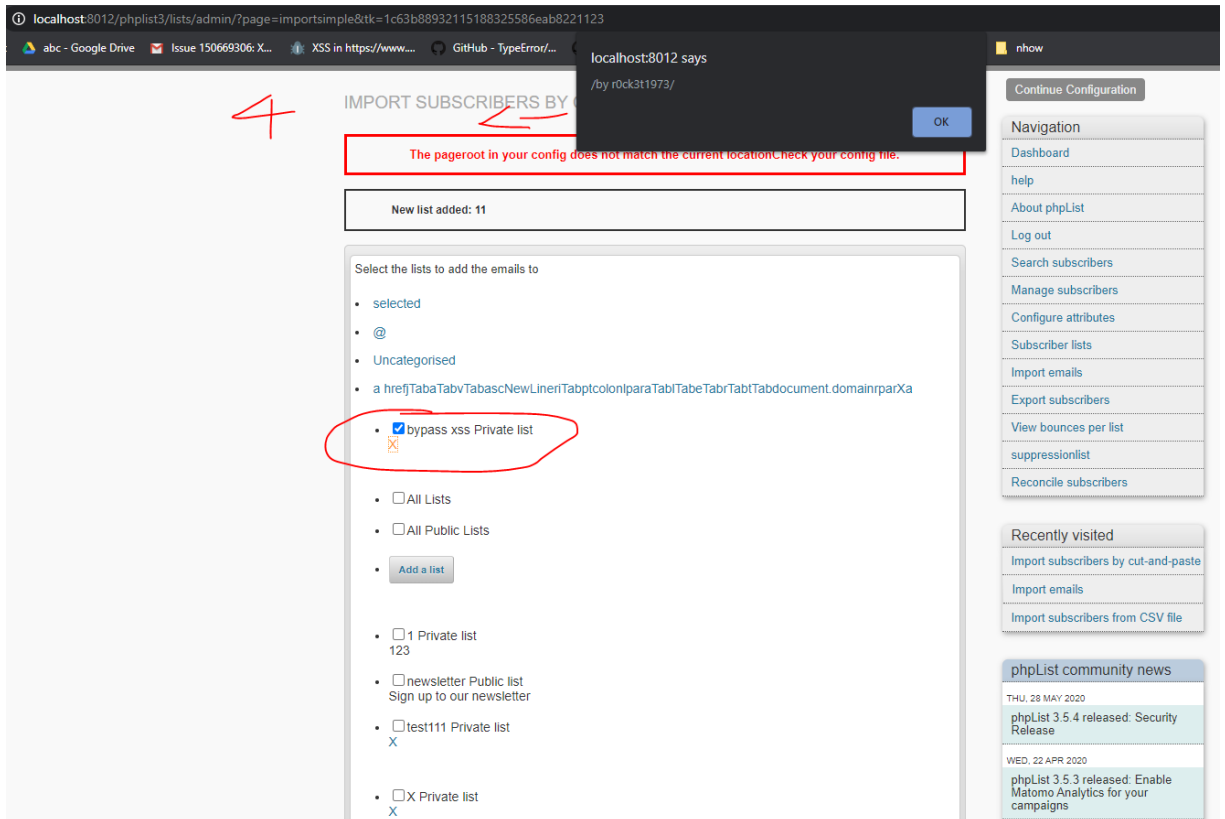
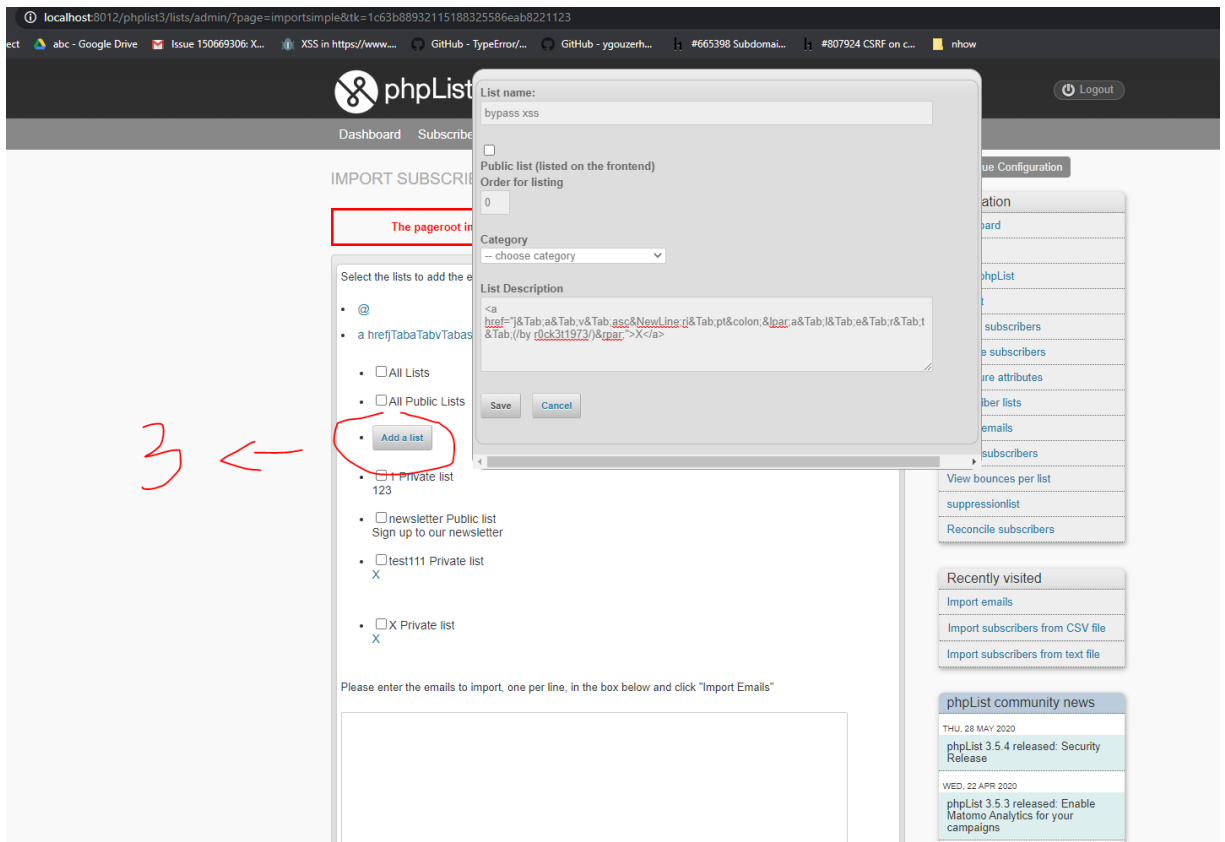
#### Recently visited

- [Import subscribers from CSV file](#)
- [Import emails](#)
- [Import subscribers from text file](#)

#### phpList community news

THU, 28 MAY 2020

phpList 3.5.4 released: Security Release



#### Also Video PoC

<https://drive.google.com/file/d/1lm42PDQ2NZW4wajwq5eh4Hx9W69jAyLc/view?usp=sharing>

#### 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!!!

r0ck3t1973 commented on May 30, 2020

Author

Payload xss  
[payload.txt](#)

Songohan22 commented on May 30, 2020

Nice... 🤔🤔🤔

michield commented on May 31, 2020


Member

I'm not sure this is a valid report. As an admin you are allowed to put HTML in the description of a list. It only fires when you click the link and doesn't fire on the loading of the page.

michield commented on May 31, 2020

Member

I'm going to close this, but feel free to comment and re-open if you disagree.

 michield closed this as completed on May 31, 2020

r0ck3t1973 commented on May 31, 2020

Author

Hi @maltfield  
Are you sure it is not a valid report? I tried inserting payload on some other platform and got bounty. I think you should review it!  
Tks,



maltfield commented on Jun 1, 2020

Contributor

oh hello. I think you meant to tag @michield :P

r0ck3t1973 commented on Jun 1, 2020

Author

oh, sr @maltfield :.))

michield commented on Jun 1, 2020

Member

@r0ck3t1973 Yes, that's fine, I will review.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants

