

New issue

[Jump to bottom](#)

Cross Site Scripting Vulnerability on "Send a campaign" feature in PHPList 3.5.4 #676

🔒 Closed

Songohan22 opened this issue on Jun 5, 2020 · 2 comments

Songohan22 commented on Jun 5, 2020

Describe the bug

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

To Reproduce

Steps to reproduce the behavior:

1. Log into the panel.
2. Go to `/admin/?page=send&id=3&tk=311902f27f63cc4f7466fc56ca0e916b&tab=Finish`
3. Insert payload:

```
"><img src onerror=alert(/"SonGohan22"/)>
// # "><svg/onload=prompt(/SonGohan22/)>
"><svg/onload=alert(document.domain)>
```
4. Click "Save and continue editing"
5. View the preview to trigger XSS.
6. View the preview to get in request and such Stored XSS.

Expected behavior

The removal of script tags is not sufficient to prevent an XSS attack. You must HTML Entity encode any output that is stored 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.

Screenshots

phpList :: Send a campaign - Mozilla Firefox

http://son.labs.com/admin/ X | http://son.labs.com/admin/ X | JPEG Image, 300 x 168 pixels X | +

son.labs.com/admin/?page=send&tk=311902f27f63cc4f7466fc56ca0e916b

Send a campaign

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

Choose an existing draft campaign to work on

Start a new campaign

Draft campaigns

Campaign	Entered	Age
(no title)	5 June 2020 09:07:32	9 hours 13 mins 59 seconds
(no title)	29 May 2020 22:49:10	6 days 19 hours 32 mins 21 seconds
Do you want to continue receiving our messages?	26 May 2020 10:41:23	10 days 7 hours 40 mins 08 seconds

DELETE ALL

phpList :: Send a campaign - Mozilla Firefox

phpList :: phpList :: Send X | http://son.labs.com/admin/ X | http://son.labs.com/admin/ X | JPEG Image, 300 x 168 pixels X | +

son.labs.com/admin/?page=send&id=3&tk=311902f27f63cc4f7466fc56ca0e916b&tab=

Send a campaign

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

1 Content 2 Format 3 Scheduling 4 Lists 5 Finish

Finish

Email to alert when sending of this message starts
Separate multiple with a comma

admin@gmail.com

Email address to alert when sending of this campaign has finished
Separate multiple with a comma

admin@gmail.com

☐ Add analytics tracking code

☐ Reset click statistics

☐ This is a test campaign

subject missing

Message content missing

Insert payload

phpList :: Send a campaign - Mozilla Firefox

phpList :: phpList :: Send X | http://son.labs.com/admin/ X | http://son.labs.com/admin/ X | +

son.labs.com/admin/?page=send&id=3&tk=311902f27f63cc4f7466fc56ca0e916b&tab=

Send a campaign

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

1 Content 2 Format 3 Scheduling 4 Lists 5 Finish

Finish

Email to alert when sending of this message starts
Separate multiple with a comma

// *~>svg/onload=prompt(/SonGohan22/)>

Email address to alert when sending of this campaign has finished
Separate multiple with a comma

// *~>svg/onload=prompt(/SonGohan22/)>

☐ Add analytics tracking code

☐ Reset click statistics

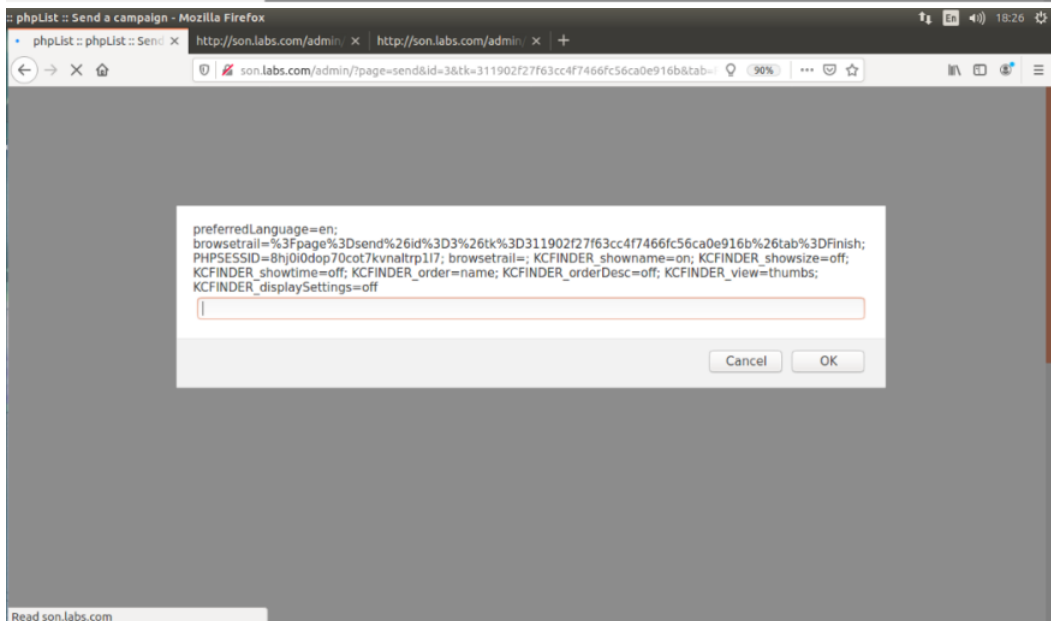
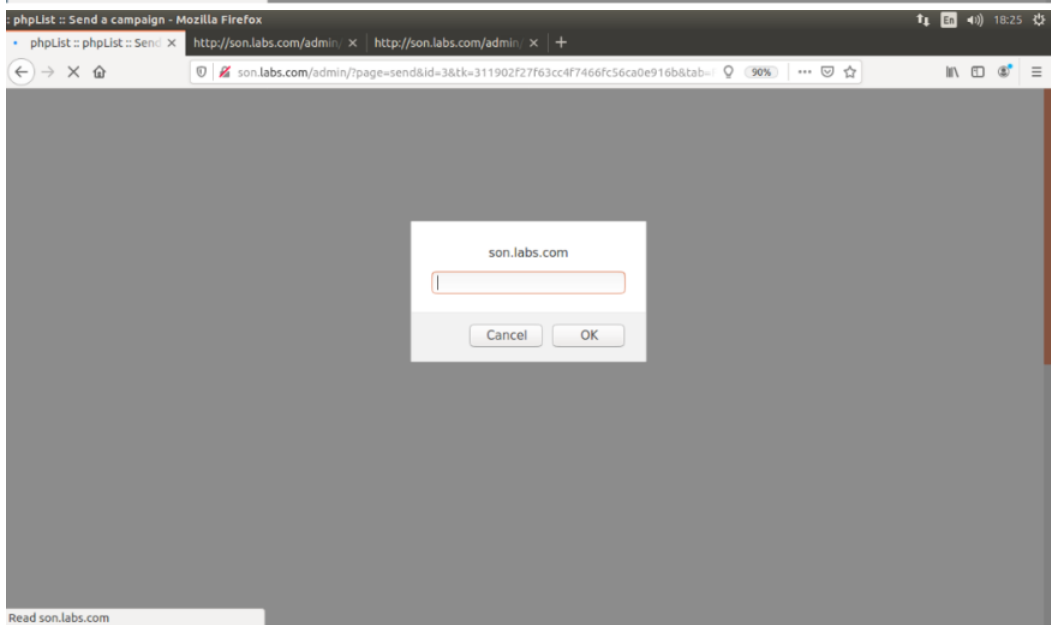
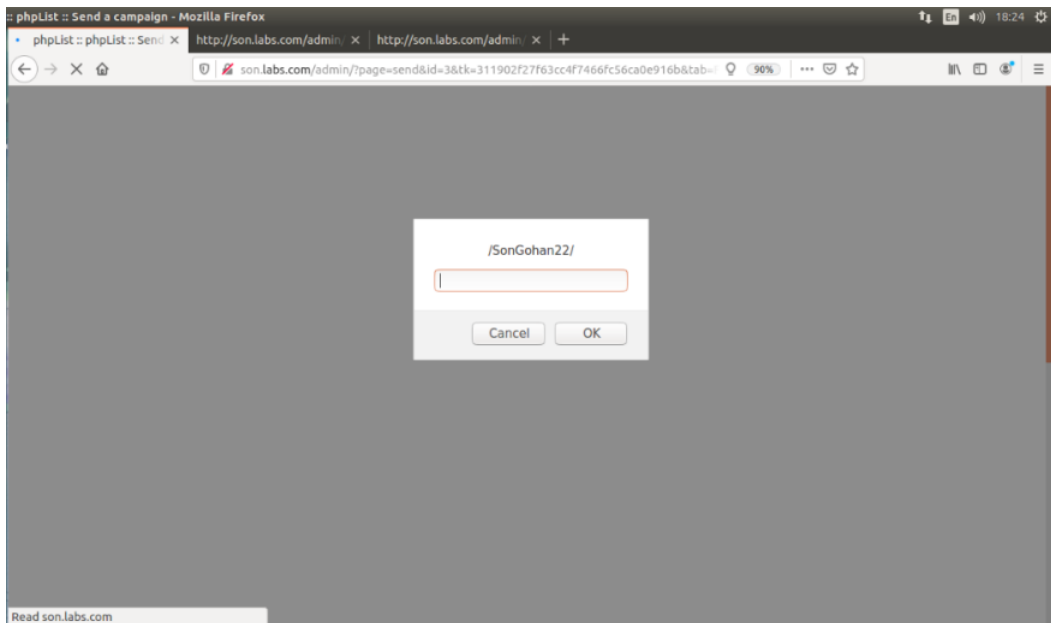
☐ This is a test campaign

subject missing

Message content missing

Some required information is missing. The send button will be enabled when this is resolved.

Trigger XSS



Desktop (please complete the following information):

- OS: Ubuntu

- Browser: Firefox
- Version: 76.0.1

Songohan22 commented on Jun 5, 2020

Author

Hi @michiield @suelaP
Please review it! Thanks

michiield commented on Jun 6, 2020

Member

Resolved with [5388df4](#)



michiield closed this as completed on Jun 6, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

