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:

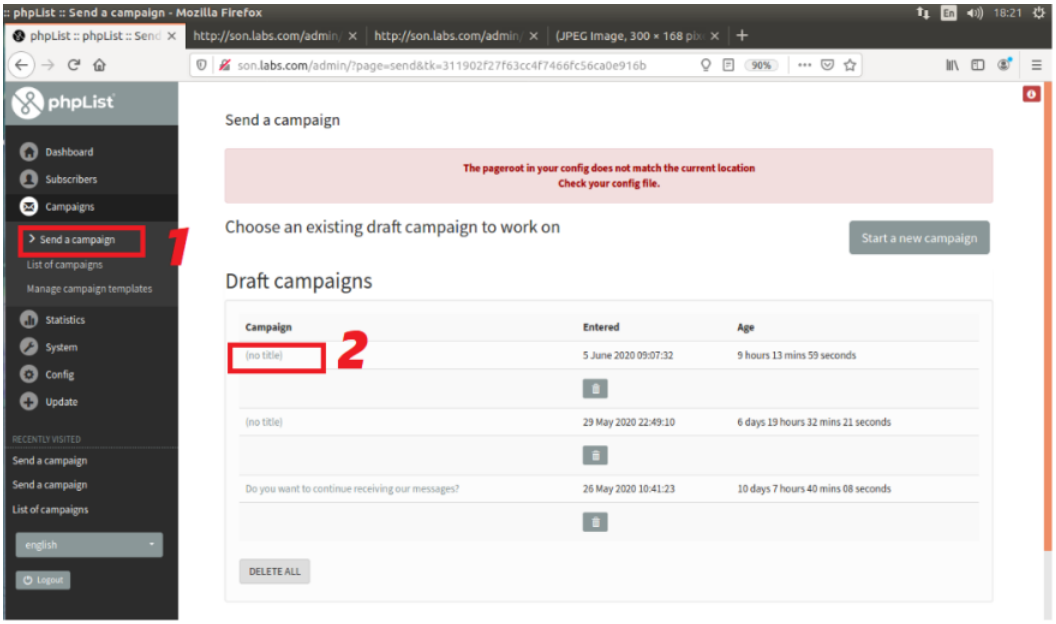
1. Log into the panel.
2. Go to "/admin/?page=send&id=3&tk=311902f27f63cc4f7466fc56ca0e916b&tab=Finish"
3. Insert payload:
   "><img src onerror=alert("SonGohan22")>

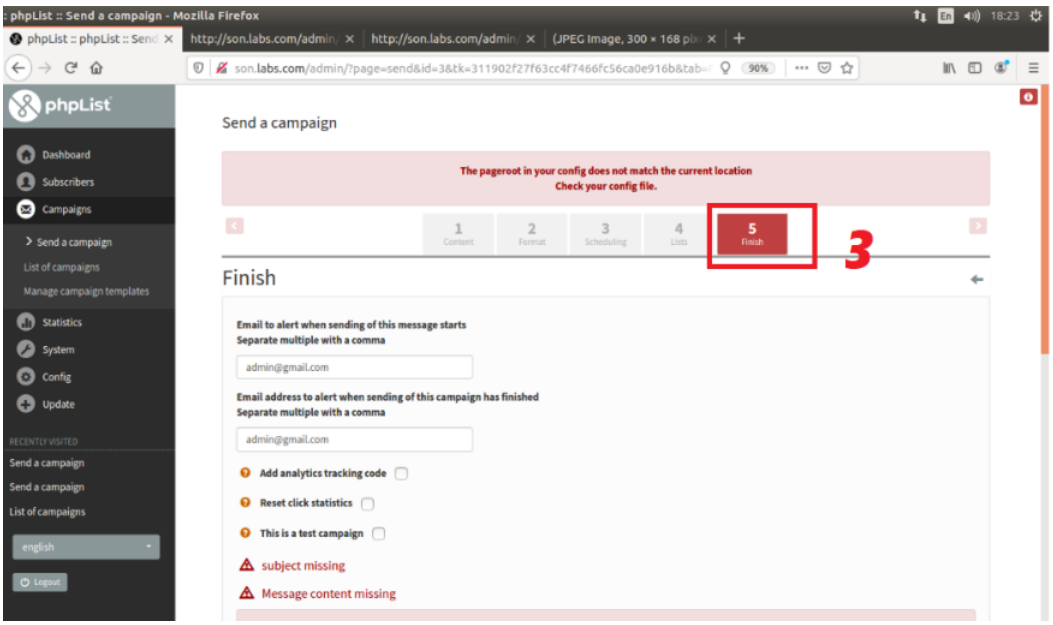
   // # "><svg/onload=prompt(/SonGohan22/)>
   "><svg/onload=alert(document.domain)>
4. Click "Save and continue editing"
5. View the preview to trigger XSS.
6. View the preview to get in request and such Stored XSS.

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.

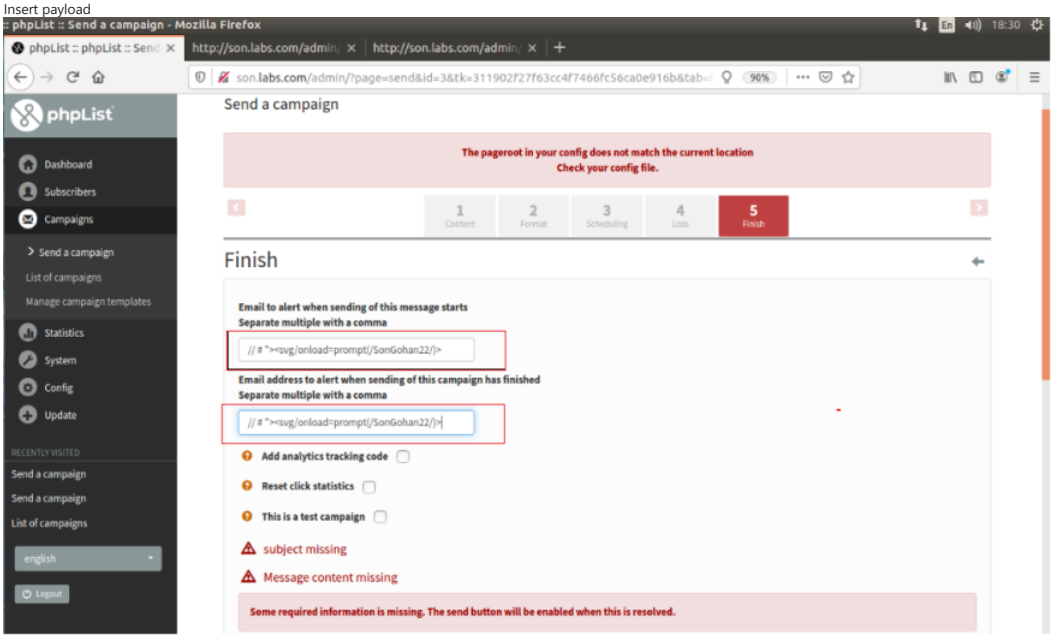
Impact
Commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

Screenshots

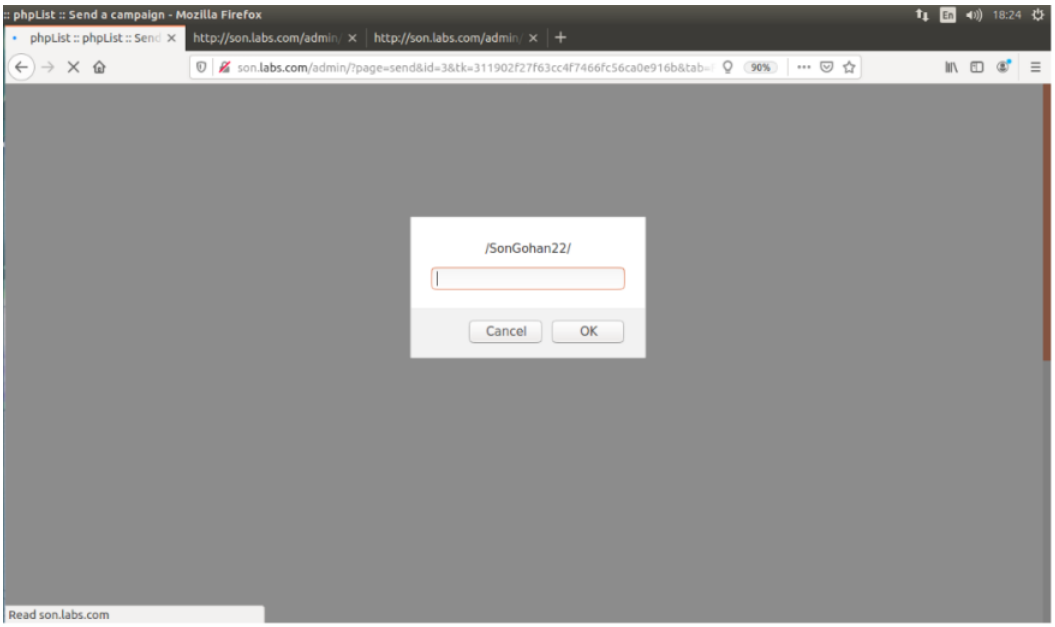


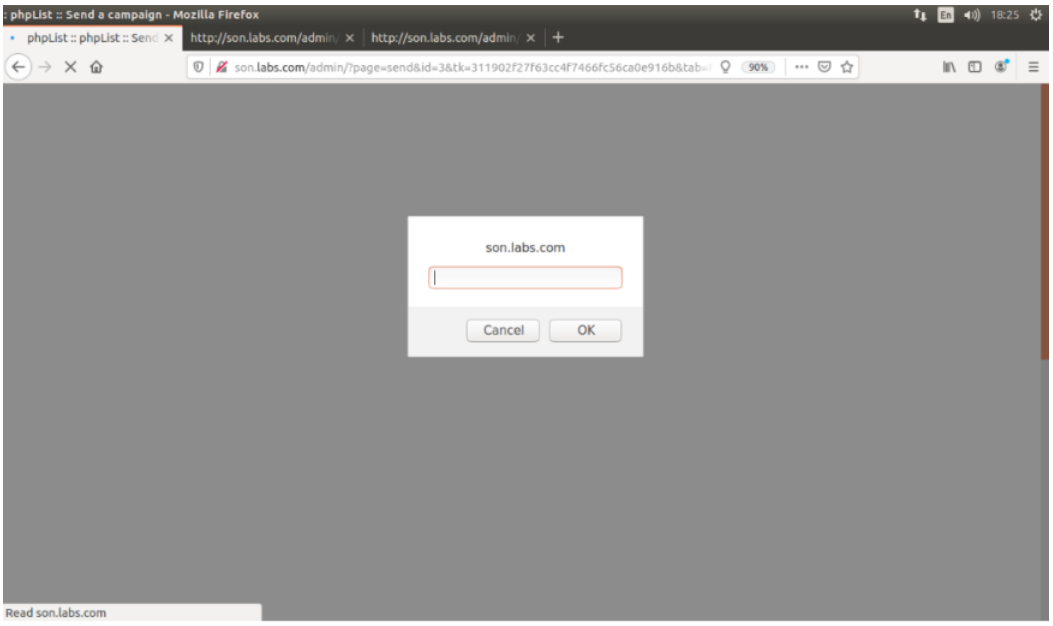


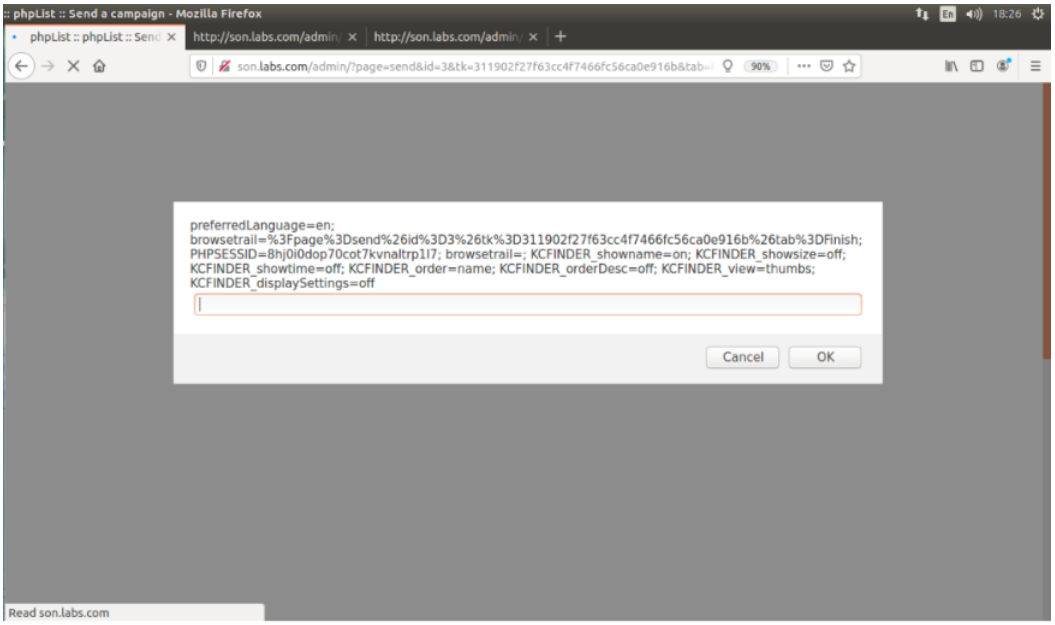
Insert payload



Trigger XSS







Desktop (please complete the following information):

- OS: Ubuntu

- Browser: Firefox
- Version: 76.0.1

Songohan22 commented on Jun 5, 2020 — Author

Hi **@michield @suelaP**
Please review it! Thanks

michield commented on Jun 6, 2020 — Member

Resolved with `5388df4`

michield 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