phpList / phplist3 Public

<> Code Issues 53 Pull requests 5 Actions Security Insights

New issue

Jump to bottom

Cross Site Script Vulnerability on "Send a Campaign" feature in phplist version 3.5.3 #665

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

r0ck3t1973 commented on May 25, 2020

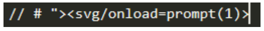
Describe the bug
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Send a Campaign" feature.

To Reproduce
Steps to reproduce the behavior:

1. Login into the panel phplist

2. Go to 'phplist3/lists/admin/?page=send&delete=5&tk=20a8f65277024ee830090611cb93e35d'

3. Click 'Start or continue a campaign' -> 'no title

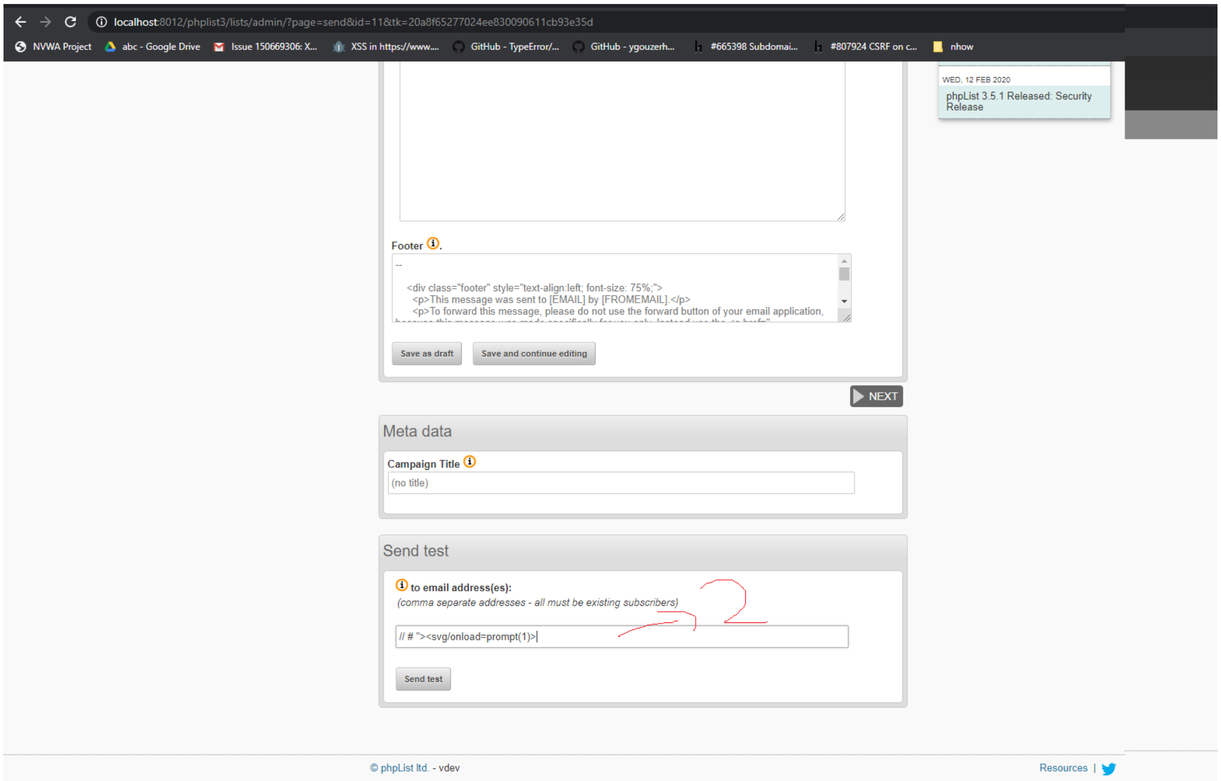
4. Insert Payload XSS: 'to email address(es)'
   // # "> <svg/onload=prompt(1)>
   
   ```
   // # "><svg/onload=prompt(1)>
   ```

5. Next

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

Screnhost



localhost:8012/phplist3/lists/admin/?page=send&id=11&tk=20a8f65277024ee830090611cb93e35d

Footer ⓘ.

```
--

   <div class="footer" style="text-align:left; font-size: 75%;">
     <p>This message was sent to [EMAIL] by [FROMEMAIL].</p>
     <p>To forward this message, please do not use the forward button of your email application,
```

Meta data

Campaign Title ⓘ

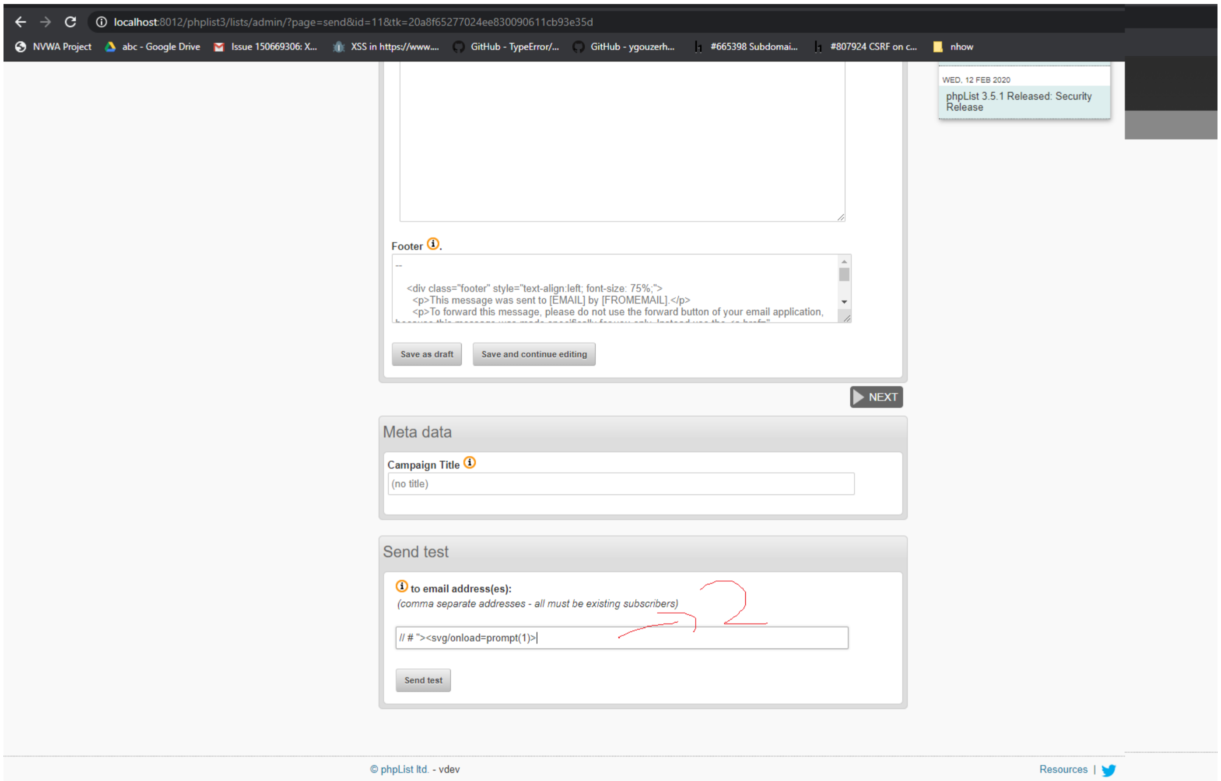
(no title)

Send test

ⓘ **to email address(es):**
(comma separate addresses - all must be existing subscribers)

```
// # "><svg/onload=prompt(1)>
```

© phpList ltd. - vdev



localhost:8012/phplist3/lists/admin/?page=send&id=11&tk=20a8f65277024ee830090611cb93e35d

WED, 12 FEB 2020
phpList 3.5.1 Released: Security Release

Footer ⓘ.

```
--

   <div class="footer" style="text-align:left; font-size: 75%;">
     <p>This message was sent to [EMAIL] by [FROMEMAIL].</p>
     <p>To forward this message, please do not use the forward button of your email application,
```

Meta data

Campaign Title ⓘ

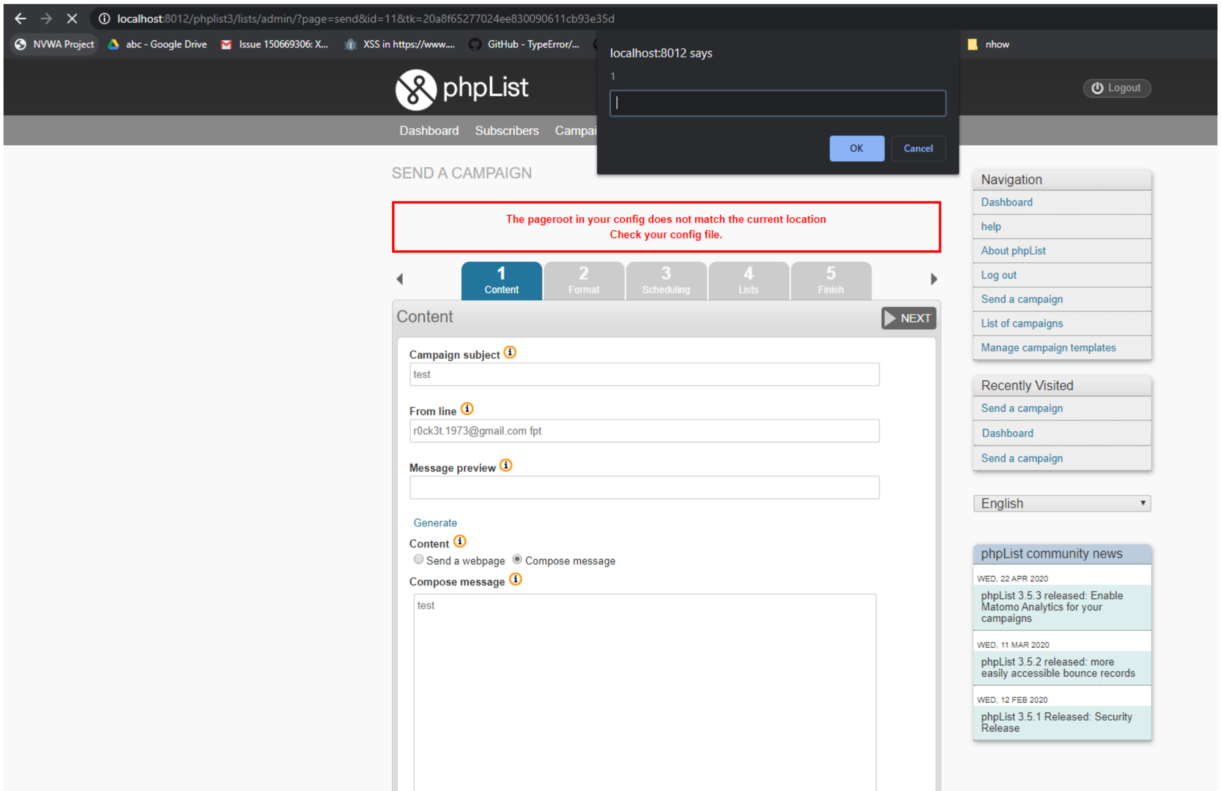
(no title)

Send test

ⓘ to email address(es):

(comma separate addresses - all must be existing subscribers)

```
// # "><svg/onload=prompt(1)>
```



localhost:8012/phplist3/lists/admin/?page=send&id=11&tk=20a8f65277024ee830090611cb93e35d

localhost:8012 says

1

SEND A CAMPAIGN

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

Content

Campaign subject ⓘ

test

From line ⓘ

r0ck3t.1973@gmail.com fpt

Message preview ⓘ

Generate

Content ⓘ

○ Send a webpage ● Compose message

Compose message ⓘ

test

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

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

suelaP commented on May 25, 2020 Member

@r0ck3t1973 thanks for your report. Unfortunately, I can not replicated the issue following the steps you provided.
The script will always be changed to "// # ">" > Not recognized as an address in the system and recognized as invalid email address when trying to add it from this page.

Can you please check again and share your findings via email: "info@phplist.com".
Thanks

r0ck3t1973 commented on May 25, 2020 Author

Hi **@suelaP**
Also Video PoC:
https://drive.google.com/open?id=1Fv5pTPIm_g344EbCybWKYp6YKSv2LRQb

suelaP commented on May 25, 2020 Member

Thanks **@r0ck3t1973**

michield commented on May 26, 2020 Member

resolved with `80250d8`

michield closed this as completed on May 26, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants