phpList / phplist3 Public

Code Issues 53 Pull requests 5 Actions Security Insights

New issue

Jump to bottom

Cross Site Scripting Vulnerability on "Bounce rules" feature in PHPList 3.5.4 #675

Closed **Songohan22** opened this issue on Jun 4, 2020 · 2 comments

Songohan22 commented on Jun 4, 2020 • edited

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

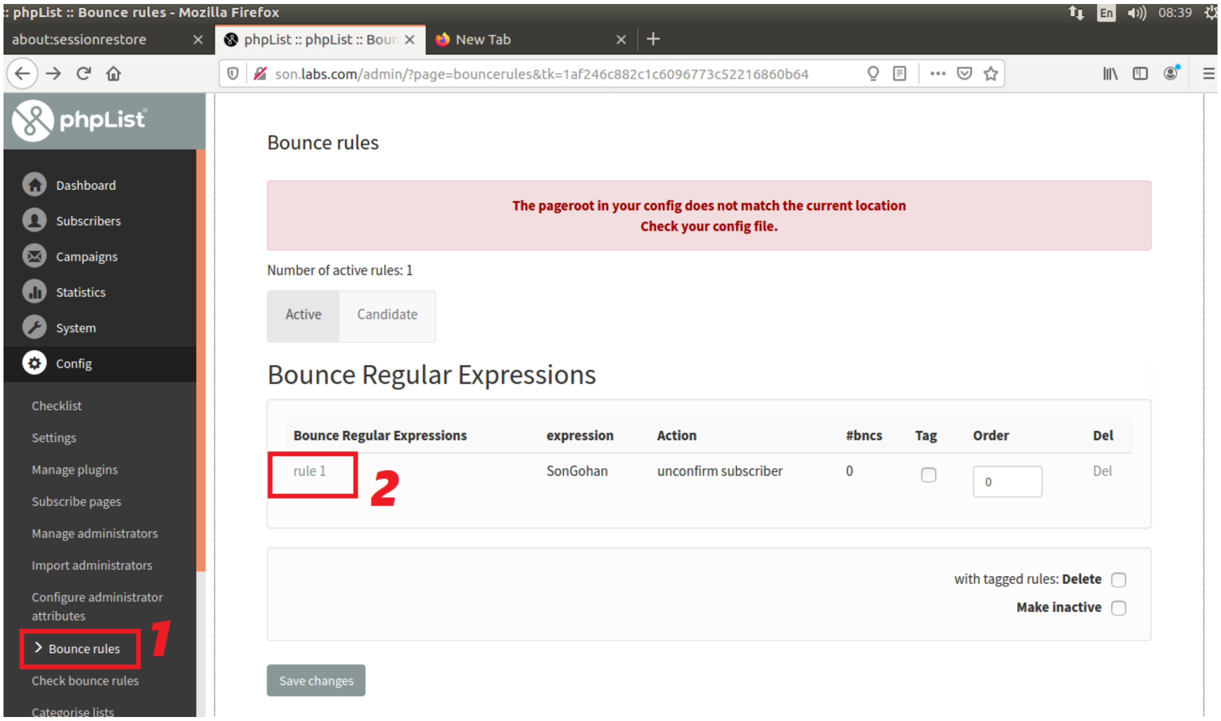
To Reproduce
Steps to reproduce the behavior:

1. Log into the panel.
2. Go to "/admin/?page=bouncerules&type=active&tk=1af246c882c1c6096773c52216860b64"
3. Click "rule1" edit infomation rule1.
4. Insert payload:
   '-alert(document.domain)-'
5. Click "Save Changes"
6. View the preview to trigger XSS.
7. 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



Bounce rules

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

Number of active rules: 1

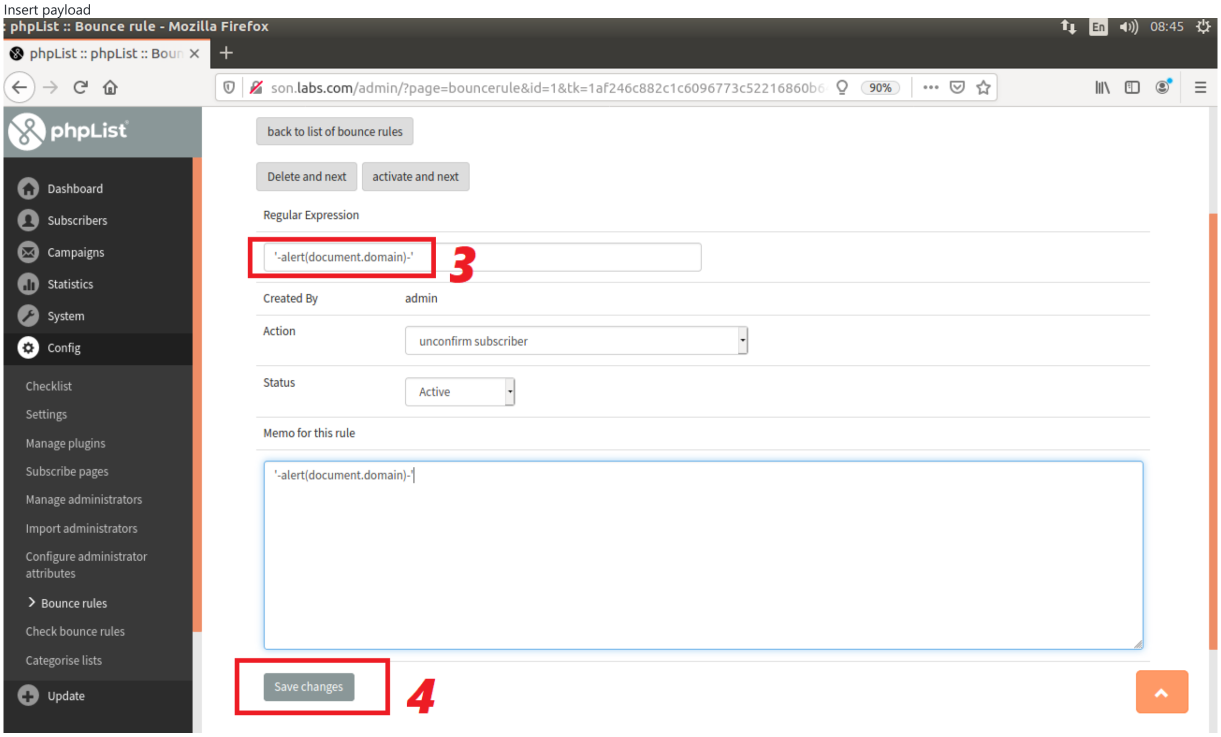
Bounce Regular Expressions

Bounce Regular Expressions	expression	Action	#bncs	Tag	Order	Del
rule 1	SonGohan	unconfirm subscriber	0	□	0	Del

with tagged rules: **Delete** □

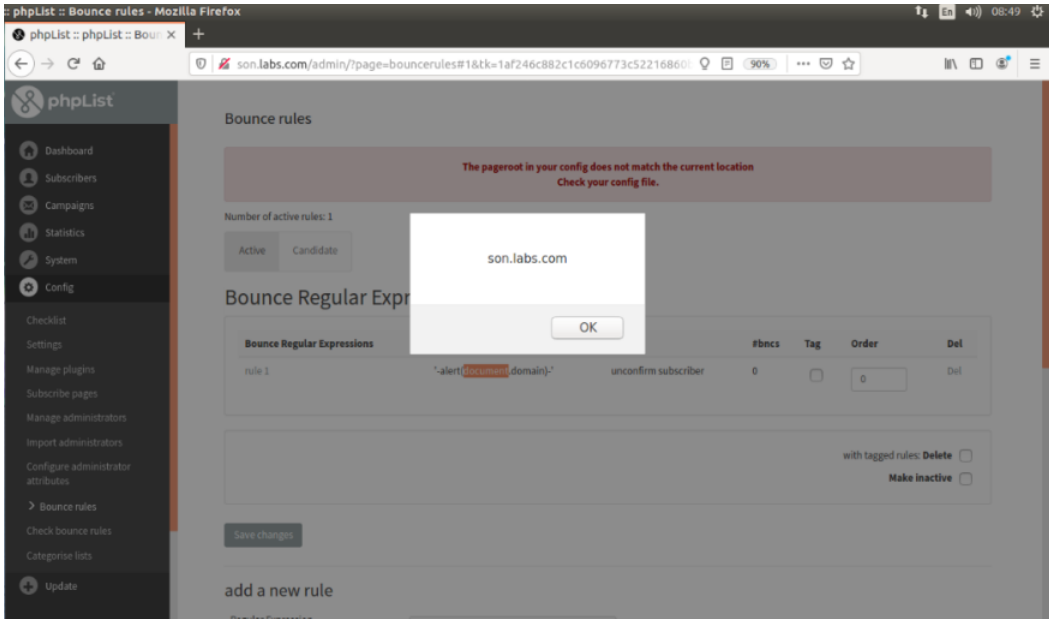
Make inactive □

Insert payload



Regular Expression	'-alert(document.domain)-'
Created By	admin
Action	unconfirm subscriber
Status	Active
Memo for this rule	'-alert(document.domain)-'

Trigger XSS



Bounce rules

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

Number of active rules: 1

son.labs.com

OK

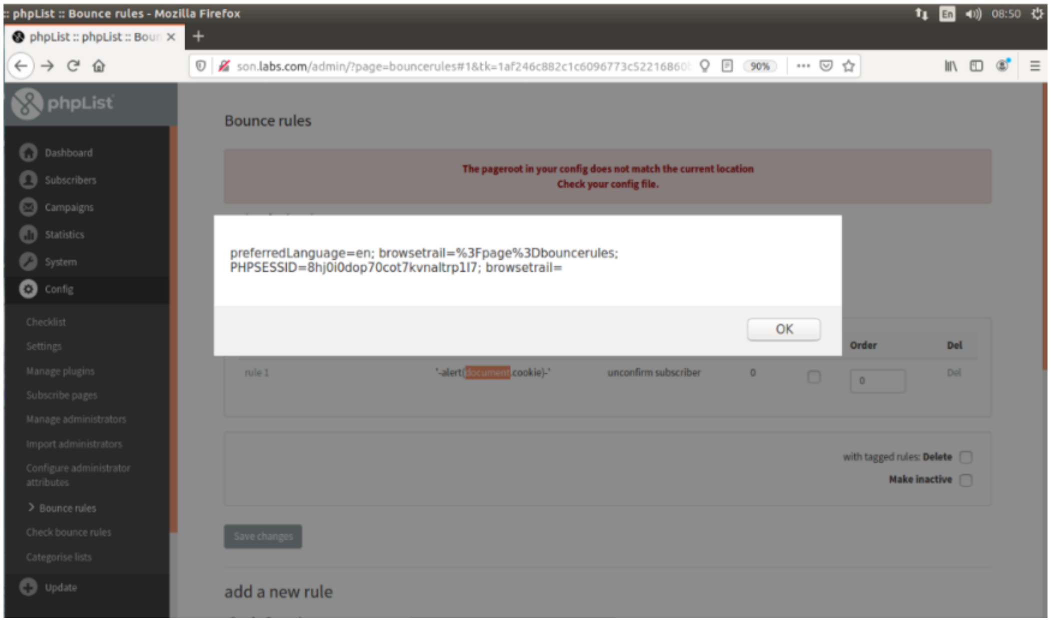
Bounce Regular Expr

Bounce Regular Expressions			#bncs	Tag	Order	Del
rule 1	'-alert(document.domain)-'	unconfirm subscriber	0	□	0	Del

with tagged rules: **Delete** □

Make inactive □

add a new rule



Bounce rules

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

```
preferredLanguage=en; browsetrail=%3Fpage%3Dbouncerules;
PHPSESSID=8hj0i0dop70cot7kvnaltrp1l7; browsetrail=
```

OK

					Order	Del
rule 1	'-alert(document.cookie)-'	unconfirm subscriber	0	□	0	Del

with tagged rules: **Delete** □

Make inactive □

add a new rule

Desktop (please complete the following information):

- OS: Ubuntu
- Browser: Firefox
- Version: 76.0.1

Songohan22 commented on Jun 5, 2020 • edited ▾ Author

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

michield commented on Jun 6, 2020 Member

Resolved with `e2b0858`

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