

New issue

[Jump to bottom](#)

## Cross Site Scripting Vulnerability on "Manage administrators" feature in PHPList 3.5.3, 3,5.4 #671

🔒 Closed Songohan22 opened this issue on May 29, 2020 · 1 comment

Songohan22 commented on May 29, 2020

### Describe the bug

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

### To Reproduce

Steps to reproduce the behavior:

1. Log into the panel.
2. Go to `/admin/?page=admins&tk=569e1f6f9e6b3a9abd9046ff57e34aaf`
3. Click "Manage administrators"
4. Click "admin" edit information admin.
5. Insert payload:  
`> <svg/onload=alert(/XSS/)>  
<img src=xss onerror=alert(1)>  
// # "> <svg/onload=prompt(/SonGohan22/)>  
6. Click "Save Changes"  
7. View the preview to trigger XSS.  
8. 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.

son.labs.com/admin/?page=admins&tk=569e1f6f9e6b3a9abd9046ff57e34aaf

phpList®

- Dashboard
- Subscribers
- Campaigns
- Statistics
- System
- Config
- Checklist
- Settings
- Manage plugins
- Subscribe pages
- > Manage administrators**
- Import administrators
- Configure administrator attributes
- Bounce rules
- Check bounce rules
- Categorise lists
- Update

RECENTLY VISITED

- Edit or add an administrator
- Manage administrators

## Manage administrators

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

Import list of admins

Add new admin

2 Administrators

Find an admin:  Go

### Administrators

Login name	ID	email	Super Admin	Disabled	Del
admin	1	admin@gmail.com	Yes	No	
Invalid email 2	3	Invalid email 2	No	No	Del

© phpList Ltd. - v3.5.4

About | Help | Resources | Twitter

son.labs.com/admin/?page=admin&start=0&id=3&tk=569e1f6f9e6b3a9abd9046ff57e34aaf

phpList®

- Dashboard
- Subscribers
- Campaigns
- Statistics
- System
- Config
- Checklist
- Settings
- Manage plugins
- Subscribe pages
- Manage administrators
- Import administrators
- Configure administrator attributes
- Bounce rules
- Check bounce rules
- Categorise lists
- Update

RECENTLY VISITED

- Manage administrators
- Edit or add an administrator
- Configure attributes

english

### Delete Invalid email 2

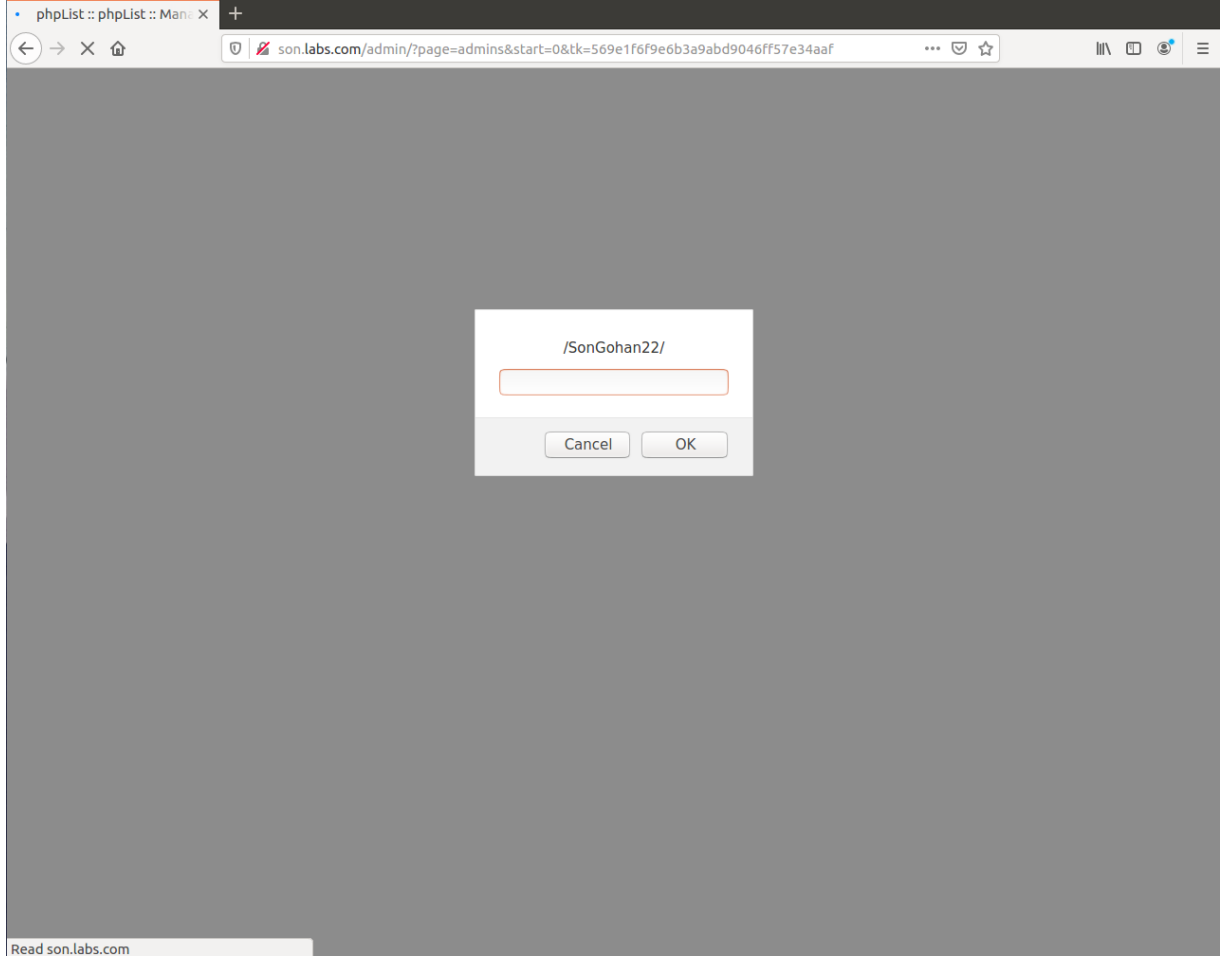
ID	3
Login name (max 25 chars)	"><svg/onclick=prompt(/SonGohan22/)>
Normalised loginname	Invalid_email_2
email	"><svg/onclick=prompt(/SonGohan22/)>
Time created	26 May 2020 12:46:07
Time modified	29 May 2020 23:19:04
Modified by	admin
Password (hidden)	Update it? <input type="radio"/> Yes <input checked="" type="radio"/> No
Last time password was changed	26 May 2020
Is this admin Super Admin?	No
Is this account disabled?	No
<?php	"><svg/onclick=prompt(/SonGohan22/)>
Privileges:	<input checked="" type="checkbox"/> Manage subscribers <input checked="" type="checkbox"/> Send campaigns <input checked="" type="checkbox"/> View statistics <input checked="" type="checkbox"/> Change settings

Save changes

© phpList Ltd. - v3.5.4

About | Help | Resources | Twitter


Click "Save Changes" -> Click "List of administrator" -> View Stored XSS




Read son.labs.com

Desktop (please complete the following information):

- OS: Windows
- Browser: Firefox
- Version: 76.0.1

 **Michield** added a commit that referenced this issue on May 29, 2020

 #671 - sanitise email address of an admin

✓ b2d581f

**Michield** commented on May 29, 2020

Member

Resolved with [b2d581f](#)

 **Michield** closed this as completed on May 29, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

