New issue

Jump to bottom

Stored XSS vulnerability in version 3.5.3 and lower #660

Closed geek-repo opened this issue on May 18, 2020 · 0 comments · Fixed by #661

geek-repo commented on May 18, 2020

XSS vulnerability exists in admin page while adding a new administrator in the Login name field.

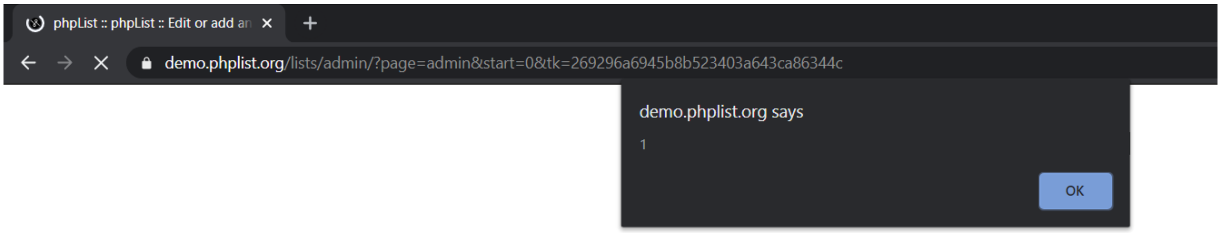
Steps to Reproduce:

1. Login as administrator
2. Navigate to the "Manage administrators" under config.
3. Click on "Add new admin"
4. Inject the payload in the Login name field

Payload: <script>alert(1)</script>

5. Enter any other required details and click on "Save changes"

POC:



phpList :: phpList :: Edit or add an

demo.phplist.org/lists/admin/?page=admin&start=0&tk=269296a6945b8b523403a643ca86344c

demo.phplist.org says

1

geek-repo changed the title ~~XSS vulnerability in version 3.5.3 and lower~~ Stored XSS vulnerability in version 3.5.3 and lower on May 18, 2020

xh3n1 mentioned this issue on May 18, 2020

Use htmlentities to output user controlled data in admin and admins pages #661

Merged

suelaP closed this as completed in #661 on May 19, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Use htmlentities to output user controlled data in admin and admins pages
phpList/phplist3

1 participant