

New issue

[Jump to bottom](#)

Stored Cross Site Scripting Vulnerability on "Users Access Groups" in rukovoditel 3.2.1 #3

✓ Closed anhdq201 opened this issue on Oct 9 · 1 comment

anhdq201 commented on Oct 9 • edited ▾

Owner

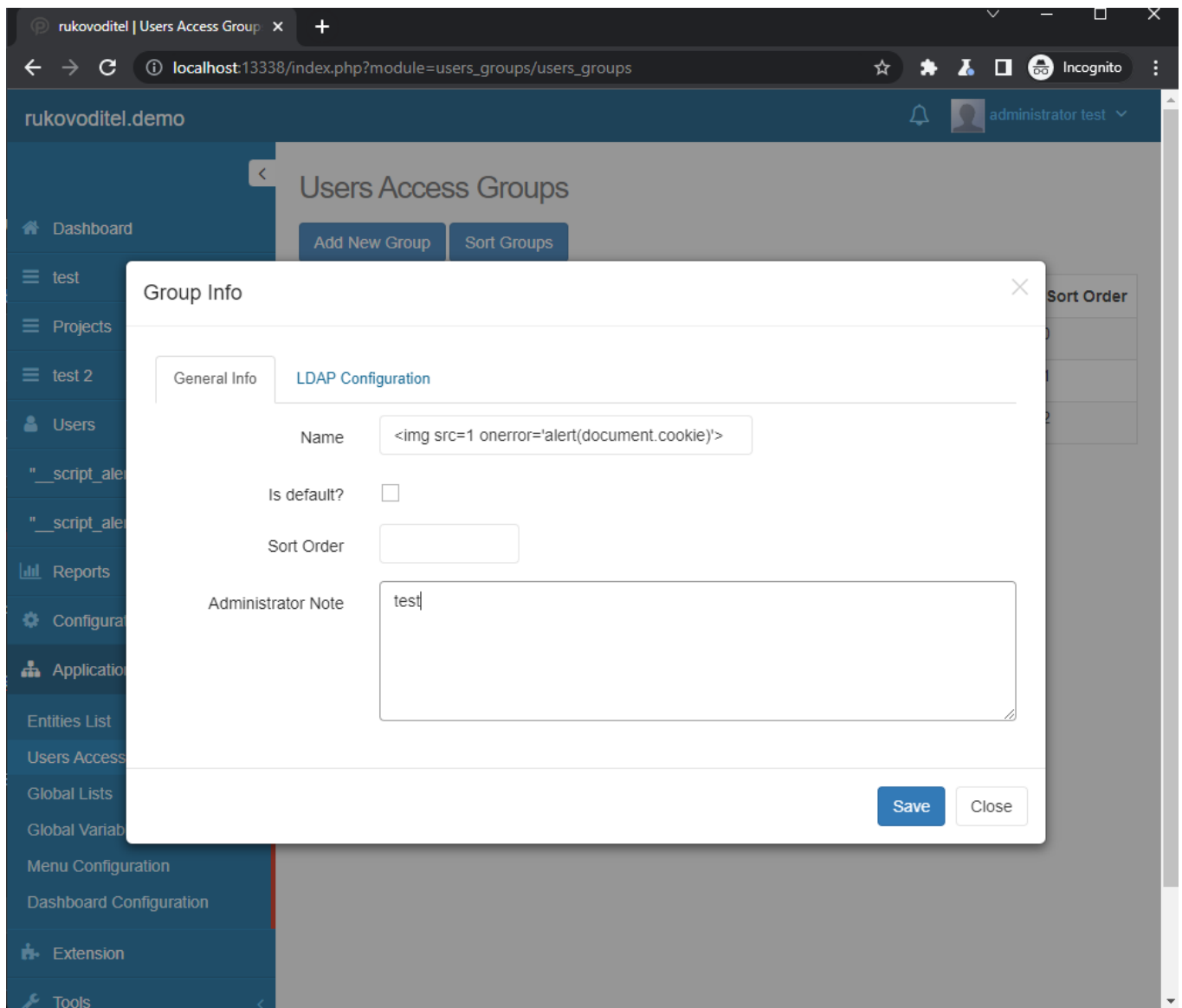
Version: 3.2.1

Description

An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Users Access Groups" feature.

Proof of Concept

Step 1: Go to `/index.php?module=users_groups/users_groups`, click "Add New Group" and insert payload `` in Name field.



Step 2: Alert XSS Message

rukovoditel | Users Access Group x +

localhost:13338/index.php?module=users_groups/users_groups

Incognito

rukovoditel.demo

localhost:13338 says

cookie_test=please_accept_for_session;
sid=nomms0shdbh9rcr934gre6grh5; user_skin=blue

OK

administrator test

Dashboard

test

Projects

test 2

Users

Application Structure

Entities List

Users Access Groups










Global Lists

Global Variables

Menu Configuration

Dashboard Configuration

Extension

Action	#	Name	Is default?	Is LDAP default?	Sort Order
 	13		No	No	0
 	6	Client	No	No	0
 	5	Developer	No	No	1
 	4	Manager	Yes	No	2

Connecting...

Impact

If an attacker can control a script that is executed in the victim's browser, then they can typically fully compromise that user.

  anhdq201 changed the title ~~test~~ Stored Cross Site Scripting Vulnerability on "Users Access Groups" in rukovoditel 3.2.1 on Oct 9

 anhdq201 closed this as completed on Oct 9

 anhdq201 reopened this on Oct 23

anhdq201 commented 24 days ago

Owner

Author

[CVE-2022-43169](#)



anhdq201 closed this as completed 24 days ago

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

