

New issue

[Jump to bottom](#)

Stored Cross Site Scripting Vulnerability on "Dashboard Configuration" in rukovoditel 3.2.1 #6

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

anhdq201 commented on Oct 9

Owner

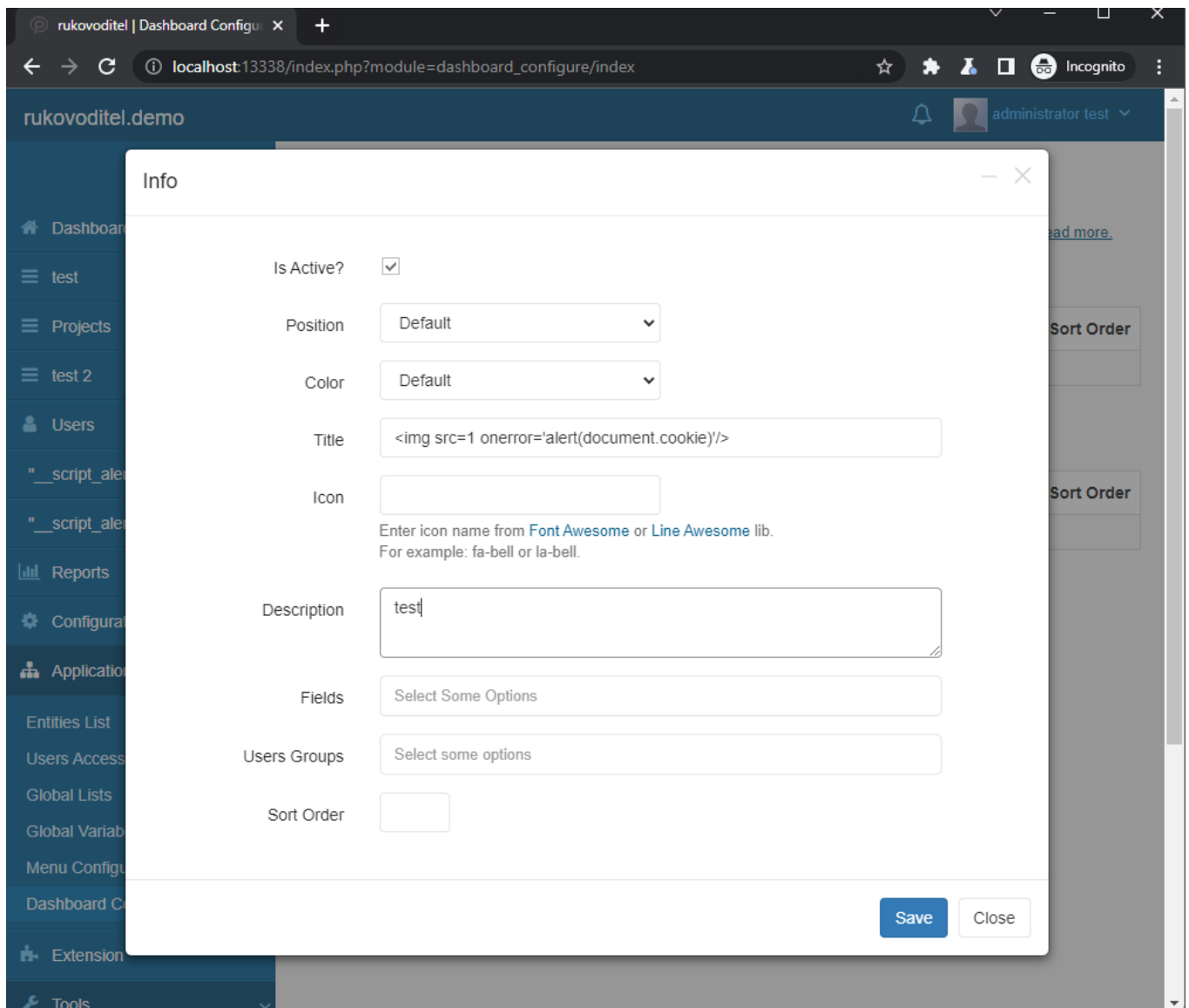
Version: 3.2.1

Description

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

Proof of Concept

Step 1: Go to "index.php?module=dashboard_configure/index", click "Add info block" and insert payload "``" in Title field.



Step 2: Alert XSS Message

rukovoditel | Dashboard Configur

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

Incognito

rukovoditel.demo

administrator test

localhost:13338 says
cookie_test=please_accept_for_session;
sid=nomms0shdbbh9rcr934gre6grh5; user_skin=blue

OK

Dashboard

test

Projects

test 2

Users

__script_alert(1)/script_

__script_alert(1)/script_

Reports

Configuration

Application Structure

Entities List

Users Access Groups

Global Lists

Global Variables

Menu Configuration



Dashboard Configuration

Extension

Connecting...

Add info block

Sections


Action	Position	Color	Title	Fields	Assigned To	Is Active?	Sort Order
 	Default	Default	test			Yes	0

Add page

Action	Color	Title	Assigned To	Is Active?	Created By	Sort Order
No Records Found						

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 closed this as completed on Oct 9

 anhdq201 reopened this on Oct 23

anhdq201 commented 24 days ago

Owner

Author

[CVE-2022-43170](#)



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

