

New issue

[Jump to bottom](#)

Stored Cross Site Scripting Vulnerability on "Global Variables" in rukovoditel 3.2.1 #5

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

anhdq201 commented on Oct 9 • edited ▾

Owner

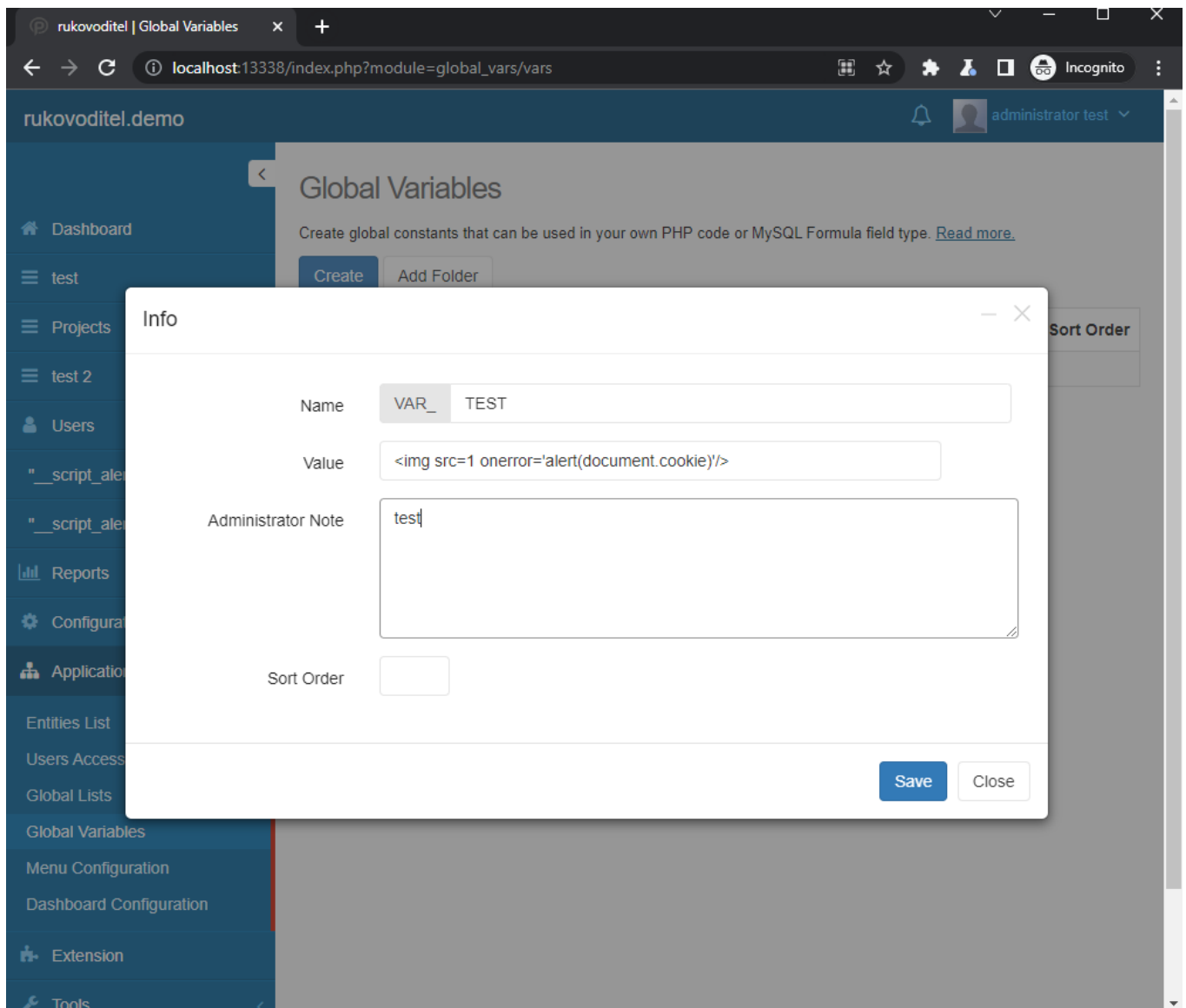
Version: 3.2.1

Description

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

Proof of Concept

Step 1: Go to `/index.php?module=global_vars/vars`, click "Create" and insert payload `` in Value field.



Step 2: Alert XSS Message

rukovoditel | Global Variables

localhost:13338/index.php?module=global_vars/vars



rukovoditel.demo

administrator test

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

OK


Create Add Folder

Action	Name	Value	Sort Order
 	<input type="text" value="VAR_TEST"/>		0

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 closed this as completed on Oct 9

 anhdq201 reopened this on Oct 23

anhdq201 commented 25 days ago

Owner

Author

[CVE-2022-43165](#)



anhdq201 closed this as completed 25 days ago

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

