

[New issue](#)[Jump to bottom](#)

Stored Cross Site Scripting Vulnerability on "Highlight row" in rukovoditel 3.2.1 #13

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

anhdq201 commented on Nov 2 · edited

Owner

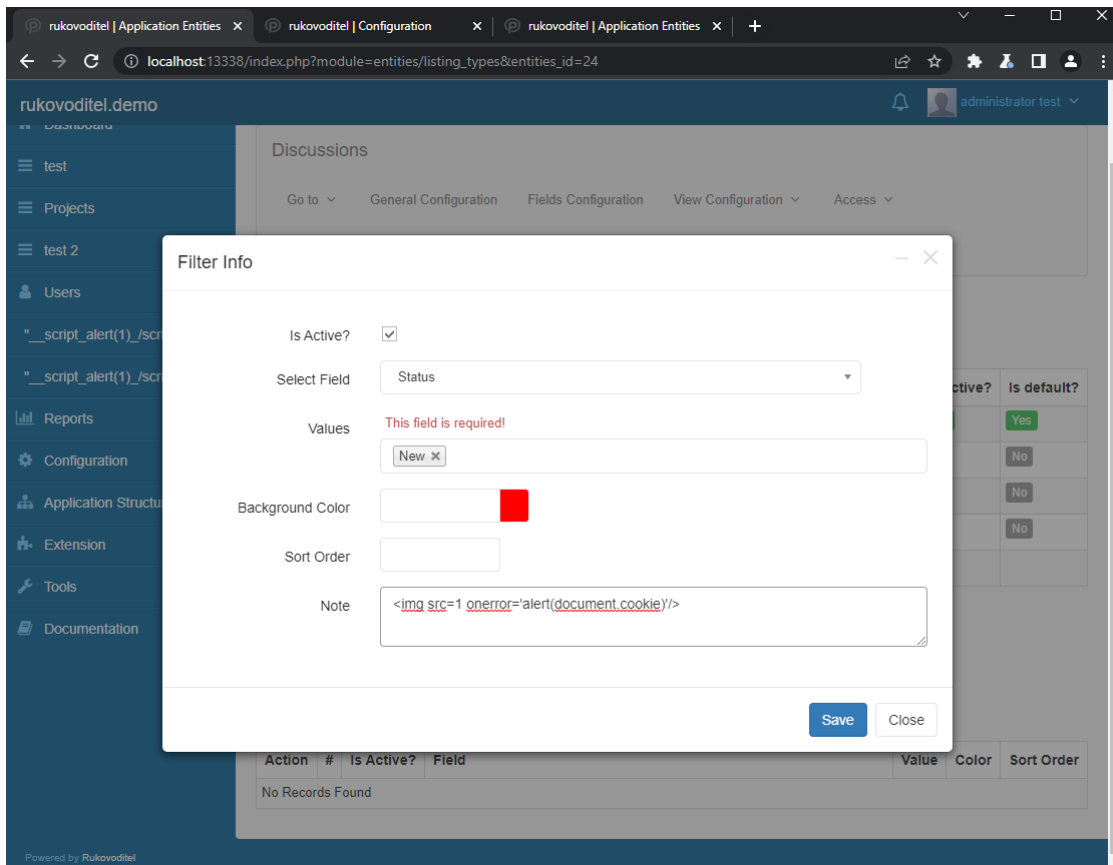
Version: 3.2.1

Description

An authenticated malicious user can take advantage of a Stored XSS vulnerability in "Note" field in the "Highlight row" feature.

Proof of Concept

Step 1: Go to `/index.php?module=entities/listing_types&entities_id=24`, click "Add" and insert payload `` in "Note" field.



Step 2: Alert XSS Message

rukovoditel | Application Entities

rukovoditel | Configuration

rukovoditel | Application Entities

+

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

rukovoditel.demo

rukovoditel demo

Dashboard

test

Projects

test 2

Users

__script_alert(1)/script_

__script_alert(1)/script_

Reports

Configuration

Application Structure

Extension

Tools

Documentation

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; fusion76811_visited=yes; userbl_results=user_joined%2Cuser_lastvisit%2Cuser_groups; userbl_status=0%2C2; userbl_search=%25; cookie_test=please_accept_for_session; __gads=ID=b63f95e1677676e3-223ed1eb6ed700-00T-1666277750-DT-1666277750-C-A1N11Mh01DmkK-w0i0767eDui

OK

Access

Listing Configuration

On this page, you can customize the appearance of the list of records. [Read more.](#)

Action	Type	Is Active?	Is default?
<input checked="" type="checkbox"/>	Table	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Tree table	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	List	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Grid	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Mobile	<input type="checkbox"/>	<input type="checkbox"/>

Highlight row

Set the field values that will highlight the entire row in the list. These rules apply to all listings. You can setup several rules and they will apply by sort order.

Add

Action	#	Is Active?	Field	Value	Color	Sort Order
<input checked="" type="checkbox"/>		<input type="checkbox"/>	State	Massachusetts		0

Connecting...

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 "Highlight row" in rukovoditel 3.2.1** to **Stored Cross Site Scripting Vulnerability on "Highlight row" in "Note" field in rukovoditel 3.2.1** on Nov 2

 **anhdq201** changed the title **Stored Cross Site Scripting Vulnerability on "Highlight row" in "Note" field in rukovoditel 3.2.1** to **Stored Cross Site Scripting Vulnerability on "Highlight row" 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

