

New issue

[Jump to bottom](#)

Stored Cross Site Scripting Vulnerability on "Fields Configuration" in "Short Name" field in rukovoditel 3.2.1

#12

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 "Short Name" field in the "Fields Configuration" feature.

Proof of Concept

Step 1: Go to "/index.php?module=entities/fields&entities_id=24", click "Add New Field" and insert payload "" in "Short Name" field.

Field Info

General Info | Is Required? | Tooltip | Access | Note

Name: test

Short Name:

Type: Input Field: Input Field

Is Heading?: ☐

Info: Simple input text field.

Use for search?: ☐

Width: Small Field

Default Value:

Hide field if value is empty: ☐

Unique Field: No

Error message: Default: The field value must be unique

Save Close

Step 2: Alert XSS Message

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-1666277760BT-1666277760C-AJNL_Mh01DmkK_v0i9k3e06i
```

OK

Add New Field With Selected

	Action	#	Form Tab	Name	Short Name	Note	Is Required?	Is Unique?	Type
<input type="checkbox"/>				ID			Yes		ID
<input type="checkbox"/>				Date Added			Yes		Date Added
<input type="checkbox"/>				Created By			Yes		Created By
<input type="checkbox"/>				test			Yes		Parent
<input type="checkbox"/>				Date Updated			Yes		Date Updated
<input type="checkbox"/>		193	Info	Status			No	No	Dropdown list
<input type="checkbox"/>		191	Info	Name	Heading		Yes	No	Input Field
<input type="checkbox"/>		192	Info	Description			No	No	Textarea with WYSIWYG edit
<input type="checkbox"/>		195	Info	Attachments			No	No	Attachments
<input type="checkbox"/>		256	Info	test			No	No	Input Field

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 "Fields Configuration" in rukovoditel 3.2.1~~ Stored Cross Site Scripting Vulnerability on "Fields Configuration" in "Short Name" field 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

