New issue

Jump to bottom

Stored Cross Site Scripting Vulnerability on "Fields Configuration" in "Name" field in rukovoditel 3.2.1 #10

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

anhdq201 commented on Nov 2 • edited Owner

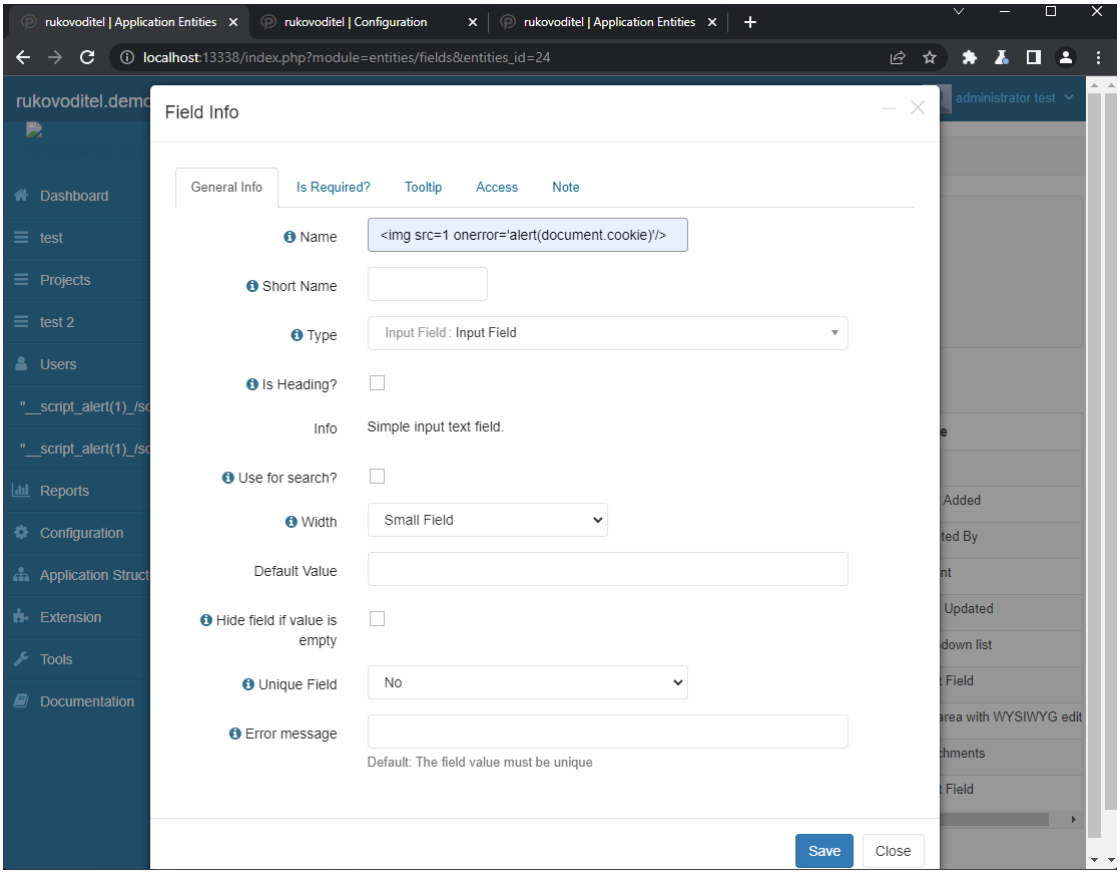
Version: 3.2.1

Description

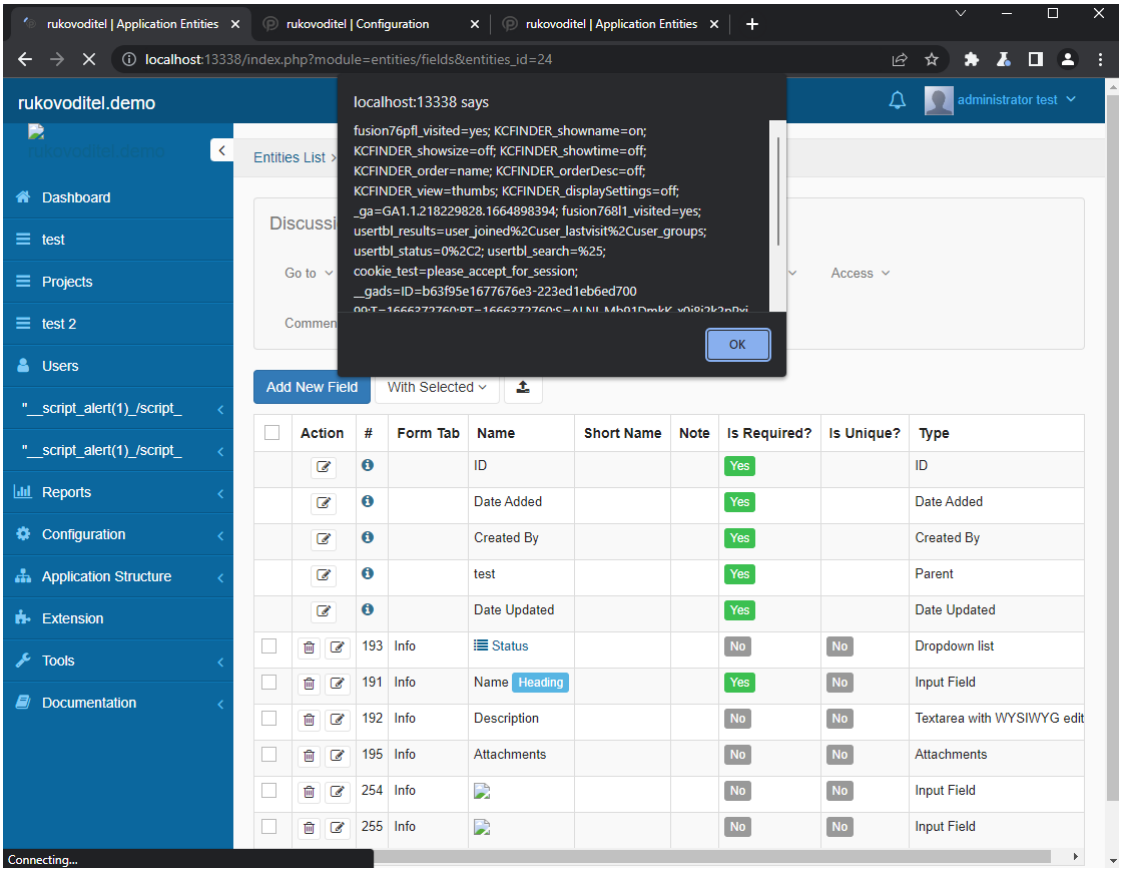
An authenticated malicious user can take advantage of a Stored XSS vulnerability in "Name" field in the "Fields Configuration" feature.

Proof of Concept

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



Step 2: Alert XSS Message



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 "Fields Configuration" in "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