

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

## Store Cross Site Scripting Vulnerability on "users\_groups" in rukovoditel 2.7.2 #2

Closed r0ck3t1973 opened this issue on Dec 15, 2020 · 1 comment

r0ck3t1973 commented on Dec 15, 2020 • edited

[Owner](#)

/Describe the bug/

I download install rukovoditel 2.7.2

An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "users\_groups" feature.

To Reproduce

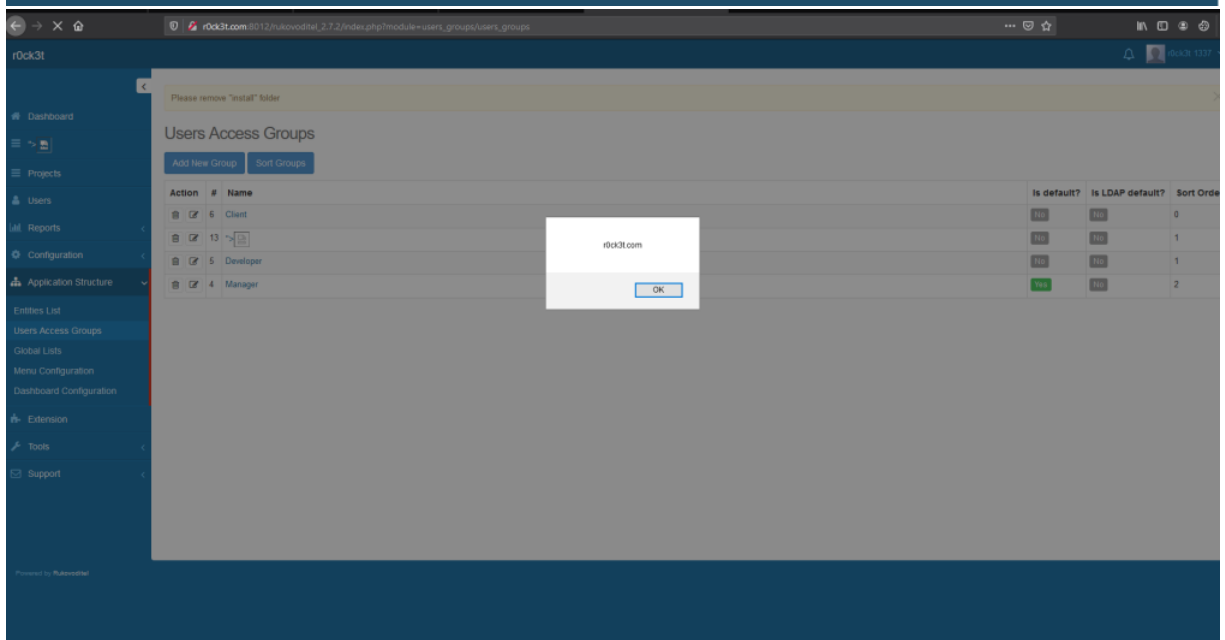
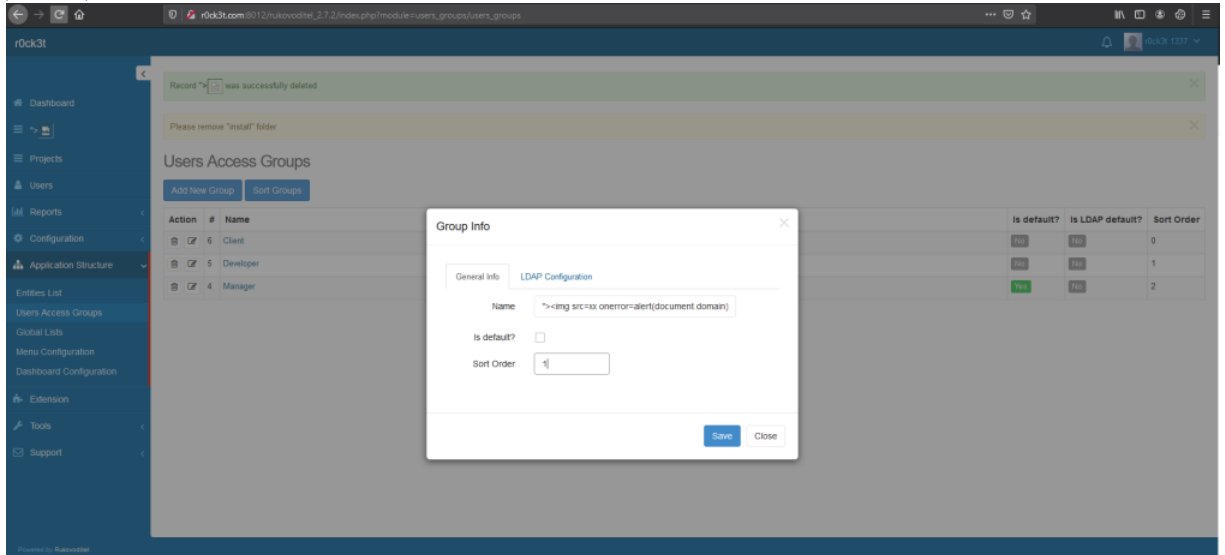
/Steps to reproduce the behavior/:

1. Login into the panel
2. Go to '/rukovoditel\_2.7.2/index.php?module=users\_groups/users\_groups'
3. Add new 'users\_groups'
4. Insert payload: "> <img src=xx onerror=alert (document.domain) >
5. Save and BOOM!!!! Alert XSS Message

/Expected behavior/

The removal of script tags is not sufficient to prevent an XSS attack. You must HTML Entity encode any output that is reflected back to the page

/Screenshots/



r0ck3t1973 commented on Jul 10, 2021

Owner Author

[CVE-2020-35986](#)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

