New issue

Jump to bottom

Store Cross Site Scripting Vulnerability on "global_lists" in rukovoditel 2.7.2 #3

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

r0ck3t1973 commented on Dec 15, 2020 Owner

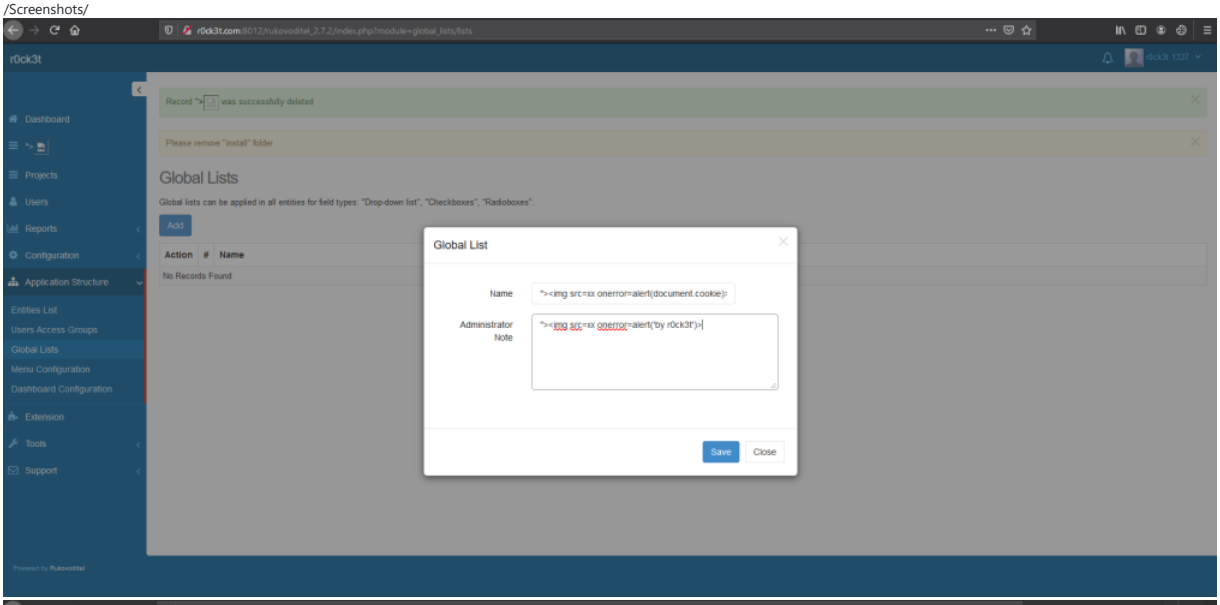
/Describe the bug/
I download install rukoviditel 2.7.2
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "global_lists" feature.

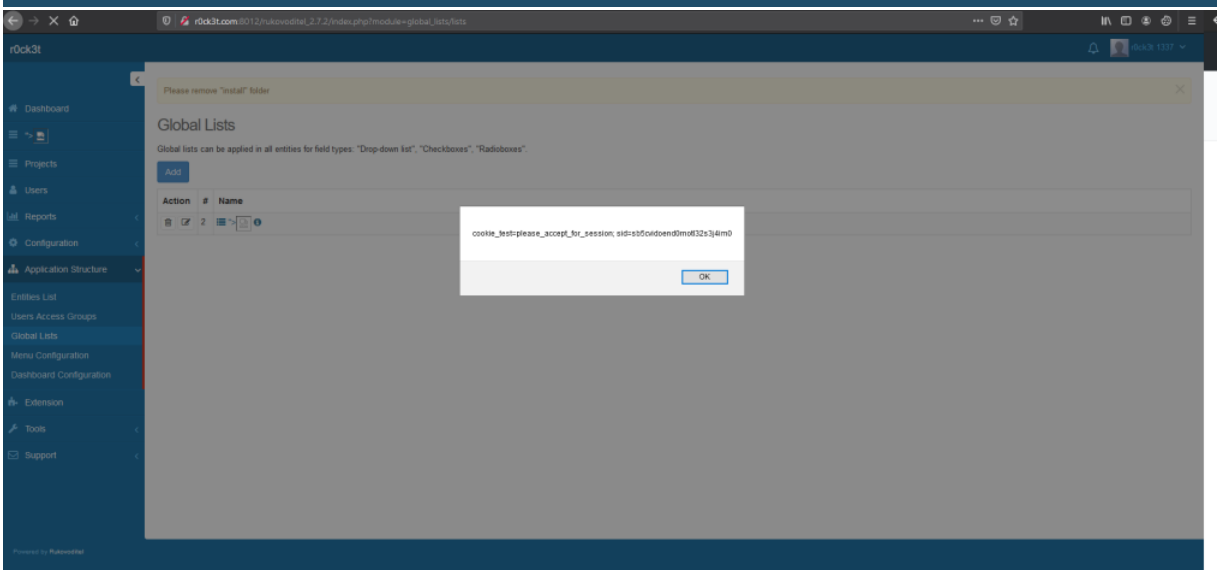
To Reproduce
/Steps to reproduce the behavior/:

1, Login into the panel
2. Go to '/rukovoditel_2.7.2/index.php?module=global_lists/lists'
3. Add new 'global_lists'
4. Insert payload: "> <img src=xx onerror=alert (document.cookie) >
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 closed this as completed on Jul 10, 2021

r0ck3t1973 commented on Jul 10, 2021 Owner Author

CVE-2020-35985

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant