New issue

Jump to bottom

# Cross Site Script Vulnerability on "Entities" in rukovoditel 2.7.2 #1

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 rukoviditel 2.7.2
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Entities" feature.

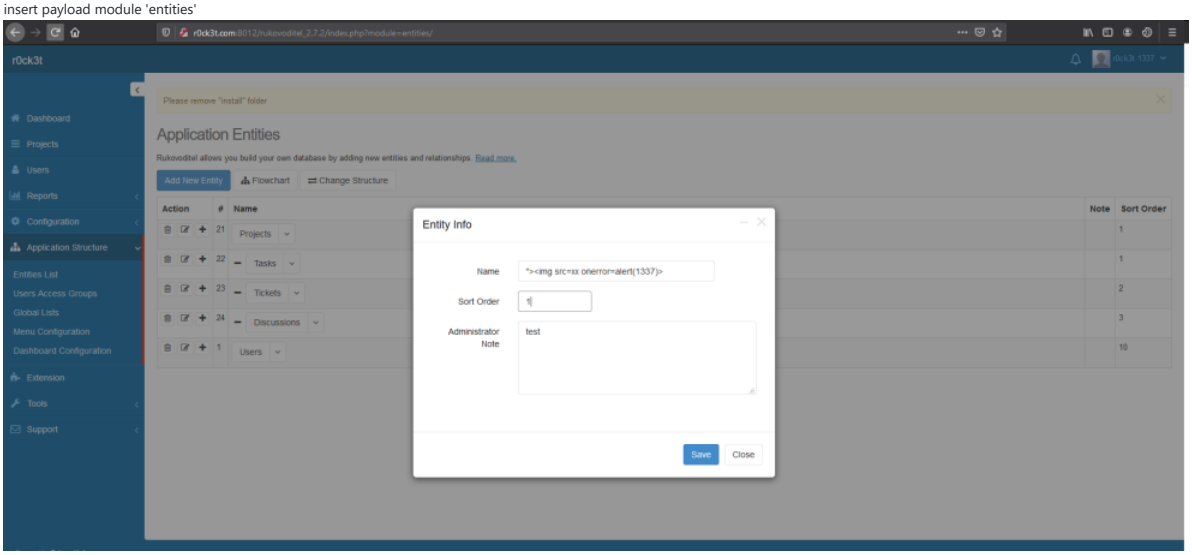
To Reproduce
/Steps to reproduce the behavior/:

1, Login into the panel
2. Go to '/rukovoditel_2.7.2/index.php?module=entities/entities'
3. Add new 'Entity'
4. Insert payload: "> <img src=xx onerror=alert (1337) >
5. Save and BOOM!!!! Alert XSS Message

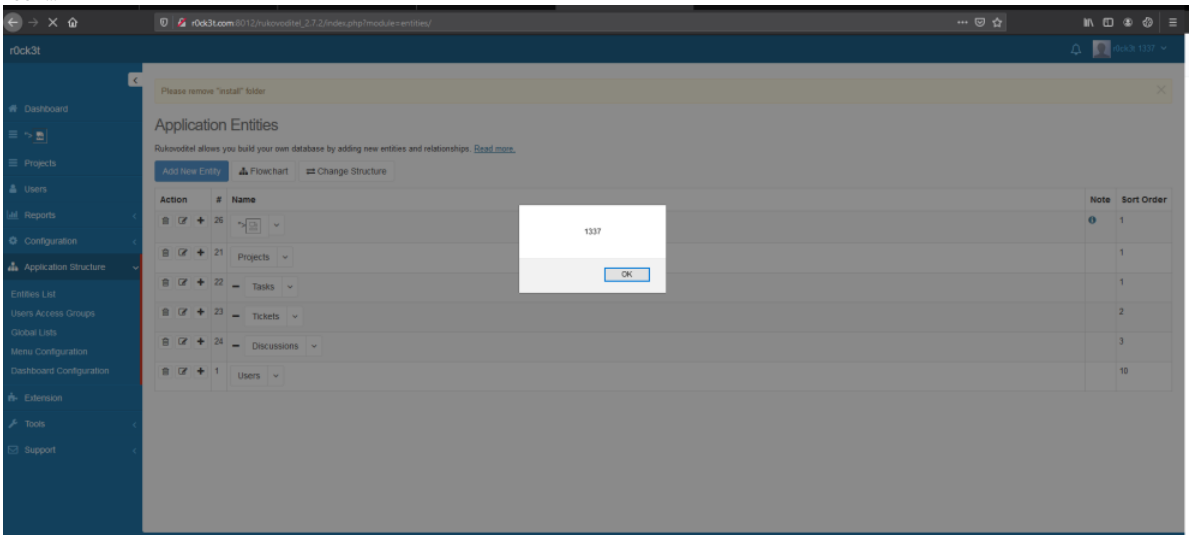
/Expected behavior/
The removal of script tags is not sufficient to prevent an XSS attack. You must HTML Entity encode any output that is reflected back to the page

/Screenshots/

1. insert payload module 'entities'




2. BOOM!!!




/Desktop (please complete the following information):/
OS: Windows
Browser: All
Version

r0ck3t1973 closed this as completed on Jul 10, 2021

r0ck3t1973 commented on Jul 10, 2021 Owner Author

CVE-2020-35987

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant