New issue

Jump to bottom

Cross Site Script Vulnerability on "Edit Menu" in Mara 7.5 #2

Open r0ck3t1973 opened this issue on Sep 1, 2020 · 0 comments

r0ck3t1973 commented on Sep 1, 2020 Owner

/Describe the bug/
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Edit Menu" feature.

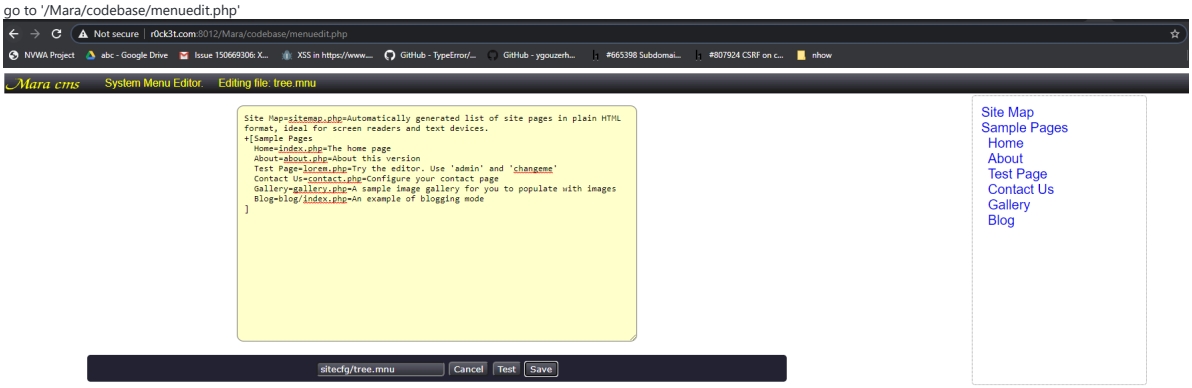
To Reproduce
/Steps to reproduce the behavior/:

1, Login into the panel
2. Go to '/Mara/codebase/menuedit.php'
3. Insert Payload:
"><**script>alert(document.domain)</script>Hello world!**
4. Click Test: Alert XSS Message
5. Save and go to Admin Panel
6. 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

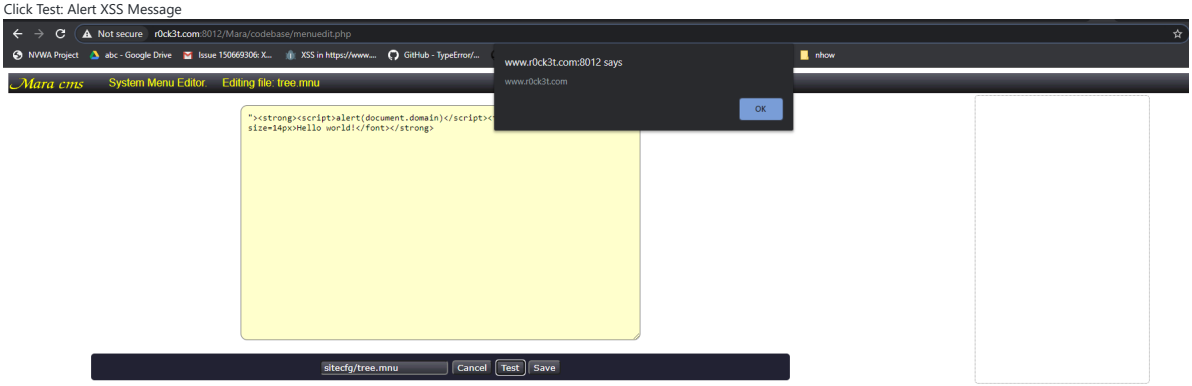
/Screenshots/

1. go to '/Mara/codebase/menuedit.php'

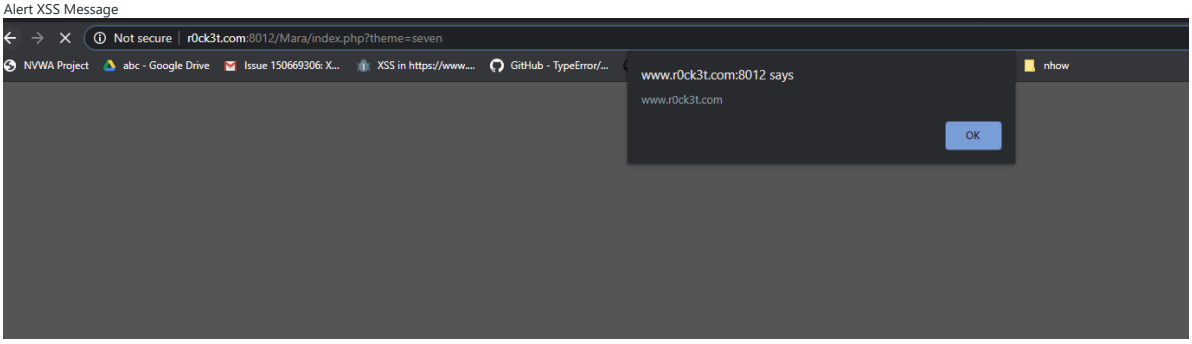


2. Insert Payload

3. Click Test: Alert XSS Message



4. Save and go to Admin Panel
5. Alert XSS Message



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

I Hope you fix it ASAP

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant