

New issue

[Jump to bottom](#)

Bypass Cross Site Script Vulnerability on "Categories" in TikiWiki version 21.4 #6

Open

r0ck3t1973 opened this issue on Jul 7, 2021 · 0 comments

r0ck3t1973 commented on Jul 7, 2021 • edited

Owner

Hi, I found stored xss in Categories.

To Reproduce

1. Login into the panel
2. Go to Documents: 'tiki-21.4/tiki-index.php'
3. Click Categories: '/tiki-21.4/tiki-browse_categories.php'
4. Create category
5. insert payload bypass xss:
`Click2`
6. Click Categories >> Click2 >> Boom alert message xss!

Impact

Commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

POC

The screenshot shows a web browser window with the URL `r0ck3t.com:8012/tiki-21.4/tiki-admin_categories.php`. The page displays the Tiki Wiki CMS groupware interface, including a sidebar menu with options like Home, Search, Contact Us, Categories, Tags, Calendar, User Wizard, My Account, Wiki, and Articles. The main content area shows a 'Success' message and a 'Category test by' section. A Notepad window titled 'changelog - Notepad' is open, displaying a changelog for Tiki Wiki CMS groupware. The changelog lists various updates and changes, including [UPD] for updates of third party/vendor libraries, [UX] for user experience improvements, [DB] for changes in the database, [MOD] for changes which may be disruptive, [REF] for refactoring, [REL] for the release process, [MRG] for branch merges, and [TRA] for translation. It also mentions that before 2.0, there was only [MOD] for both [ENH] and [MOD].

System Menu

- Home
- Search
- Contact Us
- Categories
- Tags
- Calendar
- User Wizard
- My Account
- Wiki
- Articles

test rock

Admin C

Categories

test by pass x

Test XSS Click2

changelog - Notepad

File Edit Format View Help

- * [UPD] for updates of third party/vendor libraries
- * [UX] for user experience improvements; makes Tiki easier to use and understand (more details in the changelog)
- * [DB] for changes in the database
- * [MOD] is a change which may be disruptive. For example, changing the default value of an option
- * [REF] for refactoring; changes the structure of the code (to make it cleaner or clearer), without changing the functionality
- * [REL] for the release process
- * [MRG] for branch merges, generally performed by the merge scripts
- * [TRA] for translation

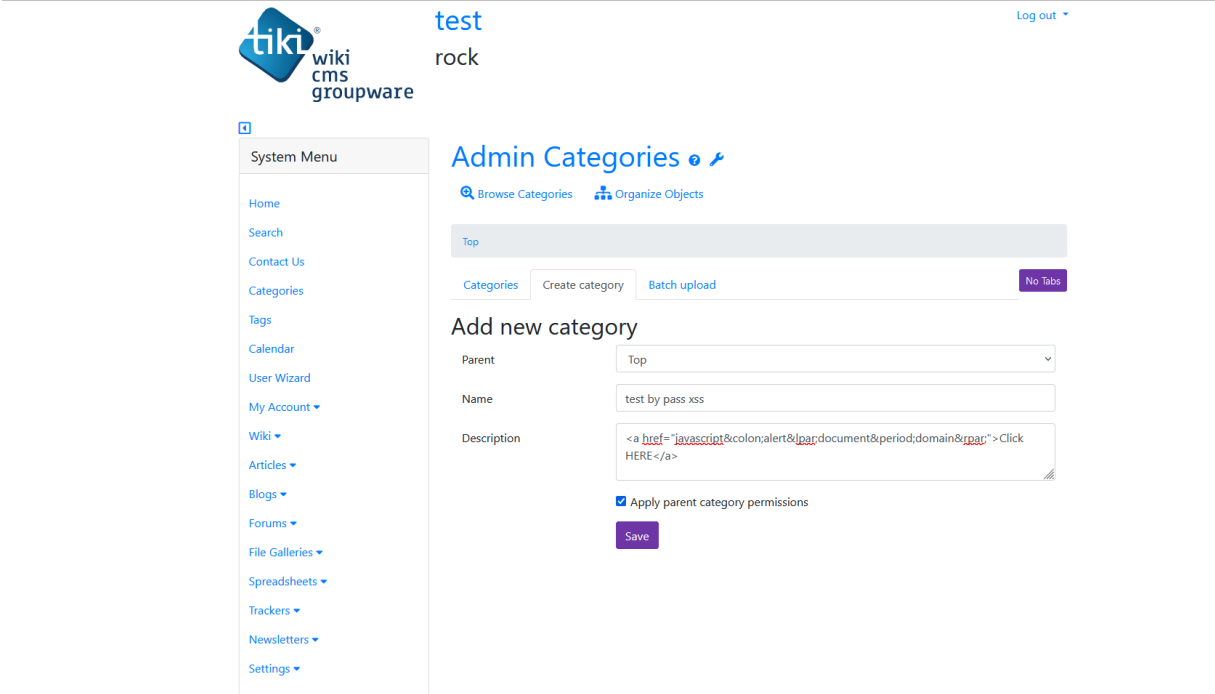
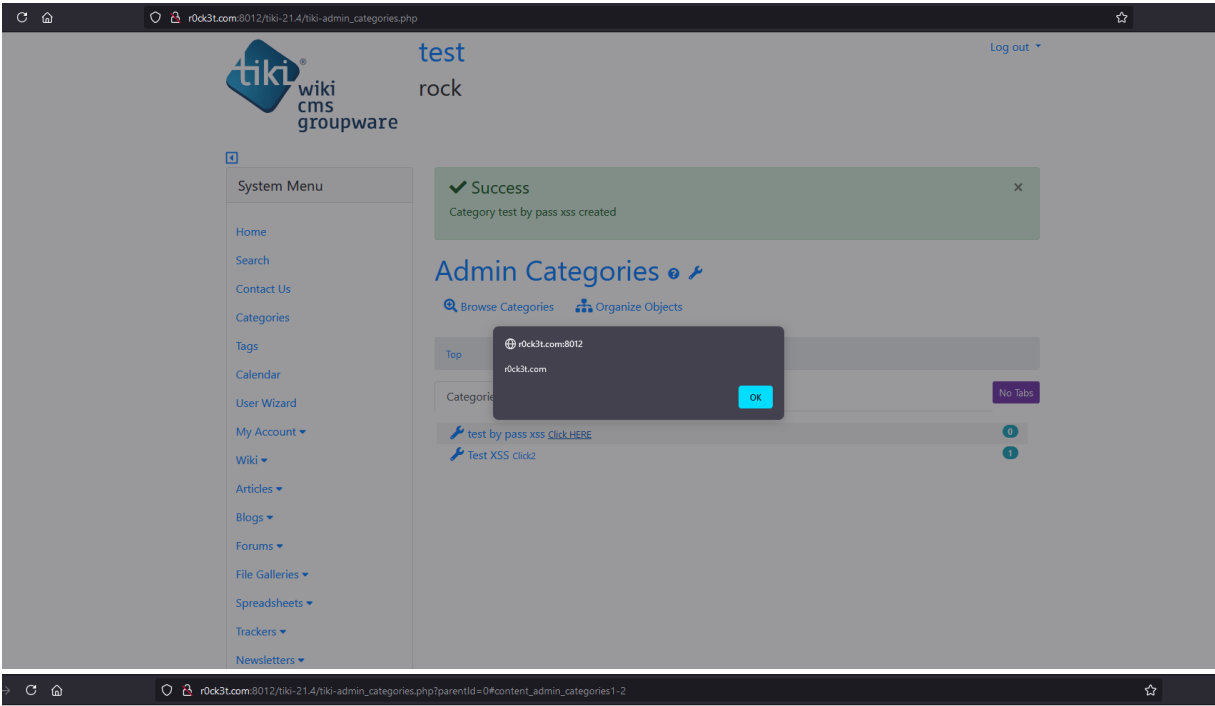
When possible, it's also nice to indicate what feature is concerned by the change. The tags info is also online: <https://dev.tiki.org/CommitTags>

Before 2.0, there was only [MOD] for both [ENH] and [MOD]:

Version 21.4
<<http://doc.tiki.org/Tiki21>>

Version 21.3
<<http://doc.tiki.org/Tiki21>>

Ln 1, Col 1 100% Unix (LF) UTF-8



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

