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

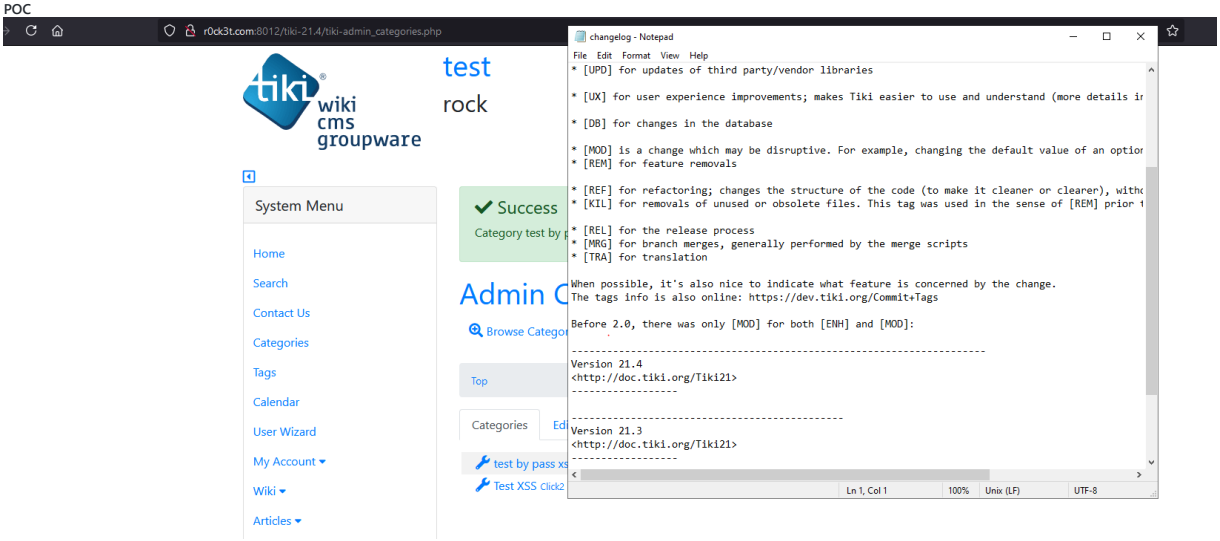
Hi, I found stored xss in Categories.
To Reproduce

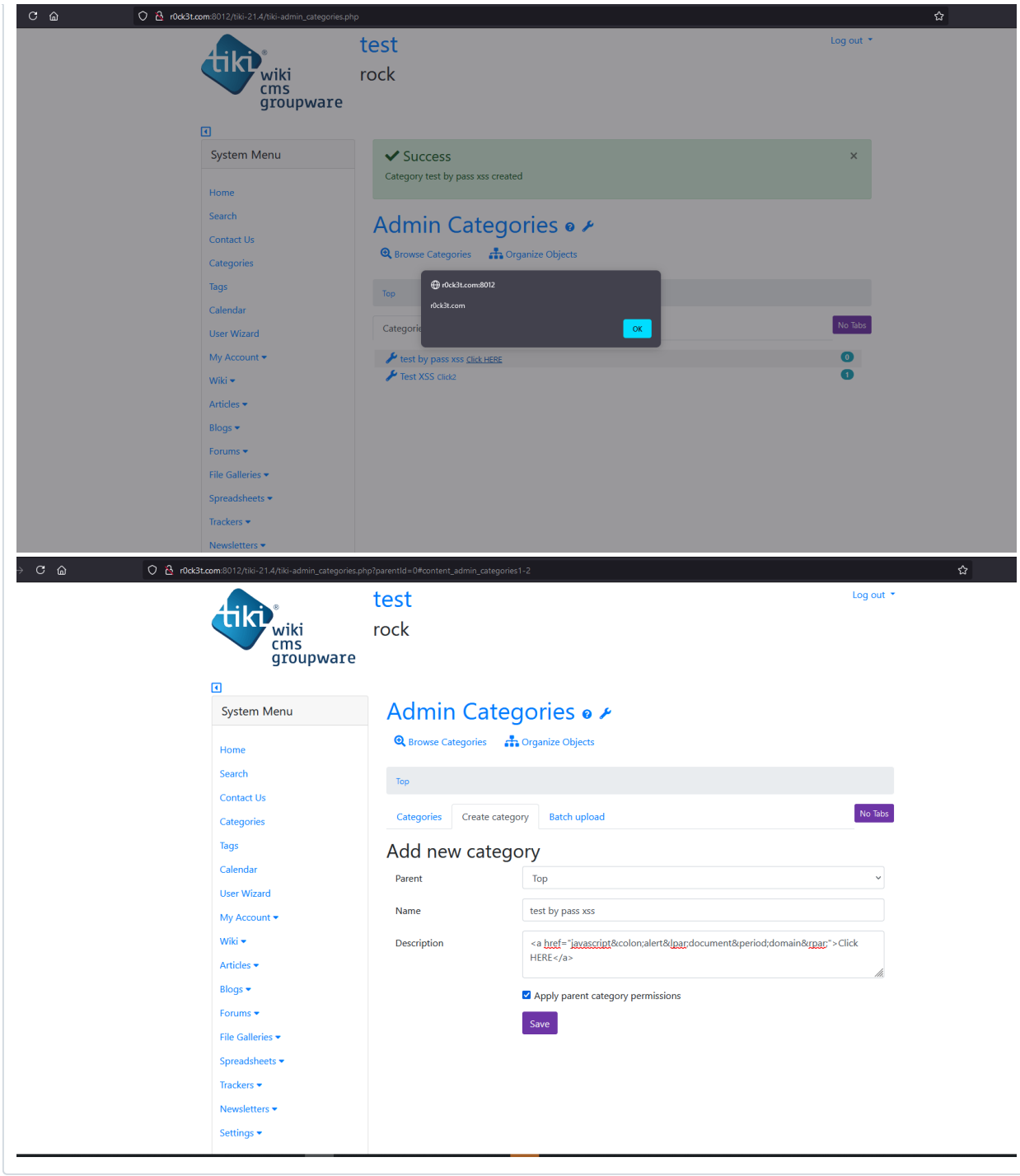
1. Login into the panel
2. Go to Documents: 'tiki-21.4/tiki-index.php'
3. Click Categories: '/tiki-21.4/tiki-browse_categories.php'
4. Create category
5. insert payload bypass xss:
   ```
   <a href="javascript&colon;alert&lpar;1337&rpar;">Click2</a>
   ```
6. Click Categories >> Click2 >> Boom alert 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





Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant