Bugs & Wish list

CSRF False positives | Tiki Wiki CMS Groupware :: Development
CSRF False positives

Status

● Open

Subject

CSRF False positives

Version

20.x

Category

- Error
- Usability
- Community projects
- Dogfood on a *.tiki.org site
- Regression

Feature

User Administration (Registration, Login & Banning)

Resolution status

New

Submitted by

Xavier de Pedro

Keep informed

lindon

Lastmod by

Xavier de Pedro

Rating

★★★★★ (0) ?

Related-to

- ⊗ Remove "Protect against CSRF with a protective step" from the login settings page
- ● CSRF Error when trying to log in from the top bar
- ● Voting in a poll gives CSRF warning.
- ⊗ CSRF on using module error messages
- ⊗ Profile preview fails with ugly CSRF error
- ● CSRF warning blocks saving menu options
- ⊗ Confirm action on CSRF warning causes warning to redisplay
- ● CSRF Error Message displayed when adding new user to group
- ⊗ elFinder: Can’t upload pictures on the tracker5 at dev.t.o (CSRF error)
- ● "The following mandatory fields are missing: Category" after anti-CSRF prompt
- ⊗ "GZip output" (feature_obzip) causes encoding errors in CSRF and error screens
- ⊗ Diagrams have poor usability still in 21.x LTS due CSRF and ticket expiration
- ◐ doc.t.o 19.x: I can't upload images to wiki pages (CSRF) with elFinder
- ● Potential cross-site request forgery (CSRF) detected. Operation blocked. Required headers are missing.

Description

A CSRF never ending loop happened to me earlier today, on dev.t.o.

I had logged in chromium-browser to dev.t.o as user "xavi" (no admin perms).

I needed to log in with my other user "xavidp" (the one with admin perms), so that I opened a private browsing window of chromium-browser. I went to visit the same page I had visited with the standard user where I had to fix some perms of that wiki page (https://dev.tiki.org/Wish%20Report%20Tpl). Clicked at "login" link at the top bar, which sent me to https://dev.tiki.org/login , provided the credentials, and then I got the message about CSRF at the url https://dev.tiki.org/tiki-login.php :

> *Error*
> *Potential cross-site request forgery (CSRF) detected. Operation blocked. Reloading the page may help.*

Every time I tried (F5, visiting somewhere else within dev.t.o) and attempting to log in, I got the same CSRF error message reproduced, and I couldn't log in as user "xavidp".

I had to open a new browser (Firefox, in this case), and login as "xavidp" was successful.

I wonder what was happening.

I tried again, at the time of reporting this issue, and I got the issue reproduced again.

FYI: I had seen other weird CSRF false positives in other contexts in a 20.x tiki I use at work (behind a firewall). I 'll keep an eye open to add more details when I hit this bug again in other use cases. But there is something wrong still in the code in 20.x.

Importance
9

Easy to solve?
4

Priority
36

Demonstrate Bug (Tiki 19+)
This bug has been demonstrated on show2.tiki.org

Demonstrate Bug (older Tiki versions)

Ticket ID
7133

Created
Sunday 21 July, 2019 17:13:12 GMT-0000
by Xavier de Pedro

LastModif
Sunday 10 October, 2021 11:36:36 GMT-0000

Comments

Doug Higby 18 Sep 19 21:32 GMT-0000

My site at lingtran.net was upgraded to Tiki 20 using a clean file base.
I have not experienced problems logging in, but I can not upload any image from disk to a wiki page without the CSRF error displaying. I have refreshed, tried different browsers, different computers, and am always blocked. The only way to upload images now is to use FTP, a major pain.

Steps to produce:
Edit a page in WYSIWYG mode.
Click on the choose or upload images button in the editor
Click on the Upload Files icon
Select an image file from your computer and upload.
Warning appears: Potential cross-site request forgery (CSRF) detected. Operation blocked. Reloading the page may help.
Refreshing does not help, nothing succeeds.

Attachments

filename	created	hits	comment	version	filetype
No attachments for this item					

The original document is available at https://dev.tiki.org/item7133-CSRF-False-positives