Bugs & Wish list

Confirm action on CSRF warning causes warning to redisplay | Tiki Wiki CMS Groupware :: Development

Confirm action on CSRF warning causes warning to redisplay

Status
Closed

Subject
Confirm action on CSRF warning causes warning to redisplay

Version
16.x Regression

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

Feature
Admin Interface (UI)

Resolution status
Fixed or Solved

Submitted by
Gary Cunningham-Lee

Volunteered to solve
lindon

Lastmod by
Xavier de Pedro

Rating
(1)

Related-to
- "The following mandatory fields are missing: Category" after anti-CSRF prompt
- CSRF False positives
- Potential cross-site request forgery (CSRF) detected. Operation blocked. Required headers are missing.
- Voting in a poll gives CSRF warning.

Description
I have "Require confirmation of an action if a possible CSRF is detected" set on tiki-admin.php?page=security. When I get the warning "Possible cross-site request forgery (CSRF, or "sea surfing") detected. Operation blocked.", and I click the "Click here to confirm your action" button, the same warning page redisplays instead of refreshing to the page where the admin action was made. This repeats as long as I keep clicking.

But the admin change does get made. If I input the admin page URL or go back in browser history to the admin page, I can see the change did take effect.

This is on my local wamp installation, so I'll need to make a show instance unless other people can reproduce this bug.

Solution
This error is from the old ask_ticket() / check_ticket() system. By Tiki17 this had been removed. Accordingly I cannot recreate in Tiki 18 or 19. Since there will be no further releases of Tiki16, there is no fix to be committed.

Also, in case this problem really relates to Tiki19, r68724 restored the default of not checking the old ticket system to avoid false anti-CSRF errors.

Workaround
Take out the ask_ticket() and check_ticket() calls from *admin/include_security.php*, although this may make the page slightly less secure.

Importance
8

Priority
40

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

SVN update

Ticket ID
6169

Created
Tuesday 08 November, 2016 04:24:55 GMT-0000
by Gary Cunningham-Lee

LastModif
Sunday 21 July, 2019 17:13:38 GMT-0000

Comments

Kailey 30 Oct 17 18:27 GMT-0000

I was wondering if anyone has found a solution to this problem, because I have run into this issue. Every time I click "confirm action" it just reloads the same page and it won't save any of my edits.

Philippe Cloutier 25 Oct 18 12:11 GMT-0000

Are you saying that every time you get a an anti-CSRF form, you get into this infinite loop? So that this is perfectly reproducible?

If so, can you provide an example list of steps to reproduce? And can you reproduce with a current version?

Philippe Cloutier 25 Oct 18 12:12 GMT-0000

Also, can you see any PHP error message (even notices, even from Smarty) which may be relevant?

Philippe Cloutier 21 Jan 19 17:16 GMT-0000

Lindon, if this should be closed, please set the Resolution status field to the appropriate value.

lindon 15 Mar 19 04:52 GMT-0000

Done, thanks Philippe.

Xavier de Pedro 21 Jul 19 17:08 GMT-0000

This 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.*

Everytime 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 successfull.

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.

Xavier de Pedro 21 Jul 19 17:14 GMT-0000

Sorry, I reopened this bug by mistake. My report is about a new bug (maybe related, but a new bug, because there is no confirmation message any more, just a CSRF message blocking the user action).
I reported a new bug report here:
https://dev.tiki.org/item7133-CSRF-False-positives

Sorry for the noise.

Attachments

filename	created	hits	comment	version	filetype

No attachments for this item

The original document is available at
https://dev.tiki.org/item6169-Confirm-action-on-CSRF-warning-causes-warning-to-redisplay

Show PHP error messages