

Redmine - Defect #13022

Image pointing towards /logout signs out user

2013-01-29 15:13 - Anonymous

Status:	Closed	Start date:	
Priority:	Normal	Due date:	
Assignee:	Jean-Philippe Lang	% Done:	0%
Category:	Security	Estimated time:	0.00 hour
Target version:	2.3.0	Affected version:	2.2.2
Resolution:	Fixed		
Description			
Creating an image with the source url /logout will automatically sign out any user.			
Code			
!/logout!			
Test case (This will sign you out!)			
See issue #13021			
This can be annoying and should be prevented by only allowing POST request with a valid CSRF token in the AccountController.logout method (source:trunk/app/controllers/account_controller.rb).			
Related issues:			
Duplicated by Redmine - Defect # 13069: XSS with images			Closed

Associated revisions

Revision 11289 - 2013-01-30 18:34 - Jean-Philippe Lang

Use POST instead of GET for logging out (#13022).

History

#1 - 2013-01-29 15:53 - Jan Niggemann (redmine.org team member)

Hi Marco,

first of all, thank you for your input and for making us aware of this.

I don't think that using a live system for demonstrating issues is neither a good idea nor good conduct.

I closed the referenced issue, but I'm not sure if deleting it wouldn't have been better...

#2 - 2013-01-29 17:05 - Anonymous

Hi Jan,

Sorry about being overly attention demanding. So, yeah sure, it is probably better to just delete the ticket.

I had actually reported this a two years ago to security(at)redmine.org, but it probably slipped through at some point. Anyway, it's just a minor annoyance, and not a real security issue.

#3 - 2013-01-29 18:20 - Etienne Massip

Maybe only respond to html format in login and logout actions?

#4 - 2013-01-29 21:50 - Jan Niggemann (redmine.org team member)

There's a security(at)redmine.org email address? Didn't know that...

#5 - 2013-01-30 08:23 - Jean-Philippe Lang

- Assignee set to Jean-Philippe Lang

- Target version set to 2.3.0

Etienne Massip wrote:

| *Maybe only respond to html format in login and logout actions?*

I've just tested this approach but it doesn't work. Using non-GET seems to be the right solution for preventing that.

#6 - 2013-01-30 18:36 - Jean-Philippe Lang

- Status changed from New to Closed

- Resolution set to Fixed

Fixed in r11289, POST is now required to logout. FTR, GET /logout will still respond with a simple logout form for compatibility, disabled-javascript support.

#7 - 2013-01-30 18:47 - Anonymous

Jan Niggemann wrote:

| *There's a security(at)redmine.org email address? Didn't know that...*

That's what it says here: [\[\[Submissions#Submitting-a-Security-Vulnerability\]\]](#)

BTW: That was fixed quickly, Kudos!