Redmine - Defect #11872

Private issue visible to anonymous users after its author is deleted

2012-09-19 02:34 - Anonymous

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Jean-Philippe Lang	**% Done:**	0%
Category:	Issues	**Estimated time:**	0.00 hour
Target version:	2.1.1		
Resolution:	Fixed	**Affected version:**	2.1.0

Description

The attached patch fixes defect #10148.

Specifically, suppose an anonymous (= not logged in) user submits an issue. Or alternatively, a user submits an issue, but later that user's account is deleted (in that case the issue is marked as submitted by anonymous).

Suppose further that the issue is marked as private. Then logged in users w/o the require permissions are not able to view the issue, as it is private.

But non-logged in users *are* able to view it. That is so because the code logic always allows the user who submitted a report to view it... Which in this particular case does not really make sense. The first part of the attached patch addresses this.

The second part fixes a minor bug in the allowed_to? method, which used to use "detect" instead of "any?", causing it to sometimes return a role object instead of a boolean.

Related issues:

Related to Redmine - Defect #10148: Private issue in public projects	**Closed**	**2012-02-03**

Associated revisions

Revision 10433 - 2012-09-19 23:48 - Jean-Philippe Lang

Anonymous users should not see private issues with anonymous author (#11872).

Revision 10437 - 2012-09-20 21:26 - Jean-Philippe Lang

Anonymous users should always see public issues only (#11872).

History

#1 - 2012-09-19 10:06 - Etienne Massip

- Tracker changed from Patch to Defect

- Subject changed from Fix: Some private issues were visible to non-logged in users to Some private issues were visible to non-logged in users

- Category set to Issues

- Status changed from New to Confirmed

- Affected version (unused) set to 2.1.0

- Affected version set to 2.1.0

Interesting, it seems there *might* be a big issue indeed if author is anonymous (is this really possible?).

I haven't tested yet (hence the conditionnal), but this issue is worth being set as Confirmed so someone will have a look to it.

Your patch lacks the covering of the 'own' issue visibility setting and the Issue.visible_condition though.

Do you have any plugin installed?

#2 - 2012-09-19 15:03 - Anonymous

- File 0001-Replace-incorrect-.detect-call-by-.any.patch added

- File 0002-Fix-bug-with-private-issues-submitted-by-or-assigned.patch added

Etienne, please take a look at #10148, which already covers this issue. Indeed, I only opened up this new report because nobody seemed to even

notice that I proposed a fix for the bug. You may want to close one of the two reports as a duplicate of the other.

And it is rather easy to confirm this bug. No plugins "required" ;) meaning I can reproduce it in a bare installation of redmine. Just setup a redmine instance allowing private issues, as well as submission by anonymous users. Submit an issue while logged out. Mark it as private. Then, try to view the issue while logged in as a non-admin, non-privileged user -- you can't, because it is private. Then log out, and voila, you can view it.

Note that a colleague of mine independently discovered the problem when we were reviewing redmine along with several other issue trackers as candidates for our new issue tracking system. I subsequently analysed it, and then found #10148, where several other people report seeing this problem, too.

You are right, the patch is not covering the 'own' issue visibility setting. I was under the impression that it does not have to, as the test for whether an issue is in "own" visibility already checks if the user is logged in. But I guess it does not hurt to add the check there, too. It's also adds some symmetry - and thus might make a future refactoring of that code easier.

I was not aware of Issue.visible_condition, oops!

The new attached patch address all of this. It also fixes another case: private issues assigned to anonymous were still shown to anon users but hidden from logged in users. However, this code really screams for some refactoring.

#3 - 2012-09-19 19:10 - Jean-Philippe Lang

With this patch, if we set the issues visibility of the anonymous role to 'own', then anonymous users won't be able to see any issues. Is that what we expect? Seems right but I just want to make it clear because it breaks a test.

#4 - 2012-09-19 21:04 - Anonymous

For what it's worth, I think that it is perfectly logical that anon users are not able to see any issues if the visibility of the anon role is set to 'own'. So I'd say the failing test should be changed (but I am even not sure how to run the test suite, so I can't submit this as a patch right now, sorry).

#5 - 2012-09-19 22:26 - Etienne Massip

I think it's nonsense to let the 'own' choice for Anonymous role and that we should remove the option from the dropdown list.

#6 - 2012-09-19 23:43 - Jean-Philippe Lang

Etienne Massip wrote:

> I think it's nonsense to let the 'own' choice for Anonymous role and that we should remove the option from the dropdown list.

Yes, and the 'all' option does not make much more sense for the anonymous role. Maybe we can simply remove the choice for this role.

#7 - 2012-09-19 23:44 - Jean-Philippe Lang

- Subject changed from Some private issues were visible to non-logged in users to Private issue visible to anonymous users after its author is deleted

- Target version set to 2.1.1

#8 - 2012-09-20 21:28 - Jean-Philippe Lang

- Status changed from Confirmed to Resolved

- Assignee set to Jean-Philippe Lang

- Resolution set to Fixed

Problem fixed in r10433 and the issues visibility option for the anonymous role is removed role in r10437 since 'all' and 'own' does not make sense for this role.

#9 - 2012-09-29 18:39 - Jean-Philippe Lang

- Status changed from Resolved to Closed

Merged into 2.1-stable.

#10 - 2012-10-11 11:31 - Anonymous

Thank you for applying this and already releasing this in 2.1.1, yay!

But may I remind you about bug #10148? I think that one should be closed now, too, as it reports the same issue.

Files

private-issues-fix.patch	1.36 KB	2012-09-19	Anonymous
0001-Replace-incorrect-.detect-call-by-.any.patch	1.12 KB	2012-09-19	Anonymous

0002-Fix-bug-with-private-issues-submitted-by-or-assigned.patch	2.08 KB	2012-09-19	Anonymous