Redmine - Defect #51

Blank screen when unauthorized access attempt.

2007-04-30 11:29 - Thomas Lecavelier

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:		**Affected version:**	

Description

When a user attempts to access an existing page without having the good permission, redmine show a blank screen instead of a explanation page as for the 404 error.

It's really painful when a user had access to a project, create issue about it and then, lose its privileges upon the project: on the "my page", it still view its issues, but get the blank screen if he try to reach them.

Reproducible: always
Steps:
1) Create a project and give permission to User A
2) User A create a issue.
3) Check that User A see the issue on "my page"
4) Withdraw permission on the project for User A
5) Reconnect User A
6) User A go to its "my page" view, click on the created issue

boom blank screen.

Log show a 403 error:

Processing IssuesController#show (for 127.0.0.1 at 2007-04-30 17:27:56) [GET]
Session ID: 407a22c49aec94478cf335a0d137e805
Parameters: {"action"=>"show", "id"=>"4",
"controller"=>"issues"}
Filter chain halted as [#<ActionController::Filters::ClassMethods::SymbolFilter:
0x4697554 @filter=:authorize>] returned false.
Completed in 0.20300 (4 reqs/sec) | Rendering: 0.00000 (0%) | DB: 0.15700 (77%) | 403 Forbidden [http://localhost/issues/show/4]

History

#1 - 2007-04-30 11:32 - Thomas Lecavelier

There's maybe a security consideration here:

If user enter an invalid reference object, he gets a clean 404 error message. If he enter a real reference object but upon which he has no right, he gets a blank screen: this means that the reference exist.

It should be better to convert the 404 error page in a generic "can't reach page" error message page whithout precision of origin, taking care of 404 and 403 HTTP error code?

#2 - 2007-04-30 15:51 - Jean-Philippe Lang

Fix committed in rev 495.
A "clean" 403 error is now displayed when trying to access a protected page.

Even if the same 404 error message was used, there would still be a way to know if a page exists:
- logout
- try to access the page
- if the page doesn't exist => 404
- if the page exist but is protected => redirected to login

form (before getting the error once logged in).

And I want to keep the auto-redirect to login...