Redmine - Defect #7750

Files/attachments can be downloaded by anyone without permissions

2011-03-01 19:42 - Stan Thorovsky

Status:	Closed	**Start date:**	2011-03-01
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Permissions and roles	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Invalid	**Affected version:**	

Description

MySQL version: 5.1.41
Ruby version: 1.8.7 (x86_64-linux)
Rails version: 2.3.5
Redmine version: 1.1

I raised this issue in the forum and was advised to submit a bug report:

http://www.redmine.org/boards/2/topics/22018

Considering that our Redmine requires authentication to access any projects it strikes me as a security hole that anyone in the world can download any files/attachments by parsing the correct URL (e.g. https://example.com/attachments/2/private_document.txt).

Since in "Roles/Permissions" Redmine allows to specify 'View Documents/Files" permission I would expect only users with that permission granted to be able to get to files and not the whole world.

Any file that we upload as "Files" or add to "Documents" can be downloaded by anyone in the world by parsing the URL directly - regardless any permissions or the fact that site requires authentication to access. Sure that 'anyone' would have to know the URL first but it is an incredibly weak protection.

Here is an example of URL that is a file in a private project in "Files" on a site that requires authentication and does not have anonymous users:

https://redmine.example.com/attachments/download/18/secretmemo.pdf

And all I need to download it is to open a terminal and type 'wget https://redmine.example.com/attachments/download/18/secretmemo.pdf'.

History

#1 - 2011-03-02 10:10 - Jean-Philippe Lang

I can not reproduce. If authentification is required OR anonymous role has not the "View Files" permission, trying to access an attachment link as an anonymous results in a redirect to the login form:

```
wget http://localhost:3000/attachments/download/399/foo.pdf
--10:08:17--  http://localhost:3000/attachments/download/399/foo.pdf
           => `foo.pdf'
Resolving localhost... 127.0.0.1
Connecting to localhost|127.0.0.1|:3000... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: http://localhost:3000/login?back_url=http%3A%2F%2Flocalhost%3A3000%2Fattachments%2Fdownload%2F399%2F
foo.pdf [following]
```

#2 - 2011-03-02 11:51 - Stan Thorovsky

Thanks for the reply, Jean-Philippe

In our case both authentication is required and 'anonymous' and 'non-member' roles do not have any permissions.

This is what I get from wget:

```
stan.t@stan.t-Inspiron-1545:~$ wget https://localhost/attachments/15/explainedFILE.png
--2011-03-02 10:31:54--  https://localhost/attachments/15/explainedFILE.png
Resolving localhost... 127.0.0.1
```

```
Connecting to localhost|127.0.0.1|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://localhost/login?back_url=https%3A%2F%2Flocalhost%2Fattachments%2F15%2FexplainedFILE.png [following]
--2011-03-02 10:32:02--  https://localhost/login?back_url=https%3A%2F%2Flocalhost%2Fattachments%2F15%2FexplainedFILE.png
Reusing existing connection to localhost:443.
HTTP request sent, awaiting response... 200 OK
Length: 3860 (3.8K) [text/html]
Saving to: `explainedFILE.png'

100%[==================================================================================================================================>] 3,860       --.-K/s   in 0s      

2011-03-02 10:32:02 (21.8 MB/s) - `explainedFILE.png' saved [3860/3860]
```

Do we have something wrong with our specific installation?

#3 - 2011-03-02 12:01 - Jean-Philippe Lang

wget saves the response to the redirect but as you can see it's a text/html response.
Please, have a look at the **content** of the file that wget saved, it should not be the png file that you requested but the html login page, even if wget saved it as explainedFILE.png.

#4 - 2011-03-02 21:09 - Stan Thorovsky

- Status changed from New to Resolved

Thank you, Jean-Philippe

It is as you say - a login page. This is very reasonable. I'll mark this "Resolved".

Thank you for your help.

#5 - 2011-03-02 23:03 - Etienne Massip

- Status changed from Resolved to Closed

- Resolution set to Invalid