Redmine - Defect #19581

_redmine_session cookie security flaw

2015-04-09 17:34 - Marcelo Dalmao

Status:	Closed	**Start date:**	
Priority:	High	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Invalid	**Affected version:**	

Description

Once logged in redmine , simply look for the cookie is generated and then use it to log in from another browser, without knowing your user name and password . It's a big security breach because anyone with access to copy the cookie , you can logging of that user without any approval of the person and without being detected.

History

#1 - 2015-04-09 19:52 - Ieuan Jenkins

If you can access a user's cookie, you'd probably have access to the credentials they posted to authenticate as well.

You should be enabling the HTTPS protocol option in the Redmine administration menu which then ensures the _redmine_session cookie is a secure cookie and cannot be intercepted.

#2 - 2015-04-10 02:50 - Toshi MARUYAMA

- Status changed from New to Needs feedback

I think it is Rails mater not Redmine.

Try Securing Redmine session cookie: _redmine_session.

source:config/application.rb#L62
From:

```
config.session_store :cookie_store, :key => '_redmine_session'
```

To:

```
config.session_store :cookie_store, :key => '_redmine_session', :secure => true
```

#3 - 2015-04-10 15:59 - Marcelo Dalmao

Thank you for your answers. The first do not think this solves the problem , but I'll try both and tell them whether or not addressed.

I explain a little better what probe done, for example we have a redmine is redmine.com , and a project called X, entered from any browser with a valid user, and access to project X. By accessing saved the contents of the cookie for use in another browser.

Open a new browser screen enter Loguin , then loaded cookie previously obtained in the new browser with content that had copied . Once you do this directly access a project X, without entering username and password.

#4 - 2015-04-10 16:30 - Toshi MARUYAMA

Redmine is Rails application.
I think you would better ask Rails community.
http://rubyonrails.org/community/

#5 - 2015-04-10 16:45 - Toshi MARUYAMA

- Subject changed from _redmien_session cookie security flaw to _redmine_session cookie security flaw

#6 - 2015-04-11 08:08 - Jean-Philippe Lang

- Status changed from Needs feedback to Closed

- Resolution set to Invalid

This is called session hijacking and it's not a Redmine or Rails security flow. That's why you should really encrypt your HTTP traffic.