Redmine - Defect #10390
Mass assignment security vulnerability

2012-03-06 18:18 - John Yani

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Code cleanup/refactoring	**Estimated time:**	0.00 hour
Target version:	1.3.2		
Resolution:	Fixed	**Affected version:**	

Description

There are many security vulnerabilities in Redmine. Some are not dangerous (such as setting created_on and updated_on fields). Some are (posting news to the project you're not allowed to).

Associated revisions

Revision 9129 - 2012-03-06 19:48 - Jean-Philippe Lang

Prevent mass-assignment when adding a news comment (#10390).

Revision 9130 - 2012-03-06 19:54 - Jean-Philippe Lang

Prevent mass-assignment when adding/updating a document (#10390).

Revision 9131 - 2012-03-06 19:59 - Jean-Philippe Lang

Prevent mass-assignment when adding/updating an issue category (#10390).

Revision 9132 - 2012-03-06 20:39 - Jean-Philippe Lang

Prevent mass-assignment when adding a project member (#10390).

Revision 9133 - 2012-03-06 20:46 - Jean-Philippe Lang

Prevent mass-assignment when adding/updating a forum message (#10390).

Revision 9134 - 2012-03-06 20:50 - Jean-Philippe Lang

Prevent mass-assignment when adding/updating a news (#10390).

Revision 9136 - 2012-03-06 21:23 - Jean-Philippe Lang

Prevent mass-assignment when adding/updating a time entry (#10390).

Revision 9137 - 2012-03-06 21:31 - Jean-Philippe Lang

Prevent mass-assignment when adding/updating a version (#10390).

Revision 9138 - 2012-03-06 21:34 - Jean-Philippe Lang

Prevent mass-assignment when adding/updating a wiki (#10390).

Revision 9139 - 2012-03-06 21:57 - Jean-Philippe Lang

Set user_id as a protected attribute (#10390).

Revision 9140 - 2012-03-06 22:36 - Jean-Philippe Lang

Prevent mass-assignment when adding/updating a forum (#10390).

History

#1 - 2012-03-06 18:19 - John Yani

Discussions:

http://www.redmine.org/boards/1/topics/29360
http://www.redmine.org/boards/2/topics/29343

#2 - 2012-03-06 23:52 - Jean-Philippe Lang

All actions for non-admin users should now be fixed.

#3 - 2012-03-07 20:34 - Jean-Philippe Lang

- Category set to Code cleanup/refactoring
- Status changed from New to Closed
- Target version set to 1.3.2
- Resolution set to Fixed

Please next time submit security issues to security at redmine dot org as requested on [[SubmittingBugs]].