Redmine - Feature #7410
Add salt to user passwords

2011-01-22 14:53 - Jean-Philippe Lang

Status:	Closed	**Start date:**	2011-01-22
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:	1.2.0		
Resolution:	Fixed		

Description

User passwords are stored as SHA1(password) which makes them vulnerable to a dictionary attack from an attacker who gets access to the database.

The change consists of generating a salt for each user and storing SHA1(salt+SHA1(password)) in the database.

Related issues:

Related to Redmine - Feature # 6394: Add Salt to Authentication	**Closed**	**2010-09-14**
Related to Redmine - Defect # 8514: Custom Password storing break pam_mysql	**Closed**	**2011-06-03**

Associated revisions

Revision 4936 - 2011-02-23 18:27 - Jean-Philippe Lang

Adds random salt to user passwords (#7410).

History

#1 - 2011-01-23 19:07 - Eric Thomas

Duplicates #6394.

#2 - 2011-02-23 18:28 - Jean-Philippe Lang

- Status changed from New to Closed

- Resolution set to Fixed

Feature committed in r4936.

#3 - 2011-04-15 09:30 - Rick I

So now if attacker gets hold of the database all he has to do is to remove leading salt (since salt is stored in DB) and proceed with the dictionary attack. I don't see how this makes password any more secure...

#4 - 2011-04-15 09:32 - Rick I

Rick I wrote:

> *So now if attacker gets hold of the database all he has to do is to remove leading salt (since salt is stored in DB) and proceed with the dictionary attack. I don't see how this makes password any more secure...*

Edit:

I take it all back. I didn't see salt+password_hash is hashed again.. my bad :F

#5 - 2020-12-08 09:32 - Go MAEDA

- Related to Defect #8514: Custom Password storing break pam_mysql added