Redmine - Feature #3155
Password policy and secure logon procedure

2009-04-10 23:44 - Vidal Arpin

Status:	New	**Start date:**	2009-04-10
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:			
Resolution:			

Description

Hi,

It would be nice if higher authentication security could be integrated in Redmine. I'd like to submit the following recommandations :

Password policy

1. use of both upper- and lower-case letters (case sensitivity);
2. inclusion of one or more numerical digits;
3. inclusion of special characters configuration choice;
4. free of consecutive identical (configurable), all-numeric or all-alphabetic characters;
5. change passwords at regular intervals (configurable) or based on the number of accesses (configurable); passwords for privileged accounts should be changed more frequently than normal passwords (configurable);
6. avoid re-using or cycling old passwords (configurable);
7. when users are required to maintain their own passwords, they should be provided initially with a secure temporary password;
8. change temporary passwords at the first log-on;
9. temporary passwords should be given to users in a secure manner; the use of third parties or unprotected (clear text) electronic mail messages should be avoided;
10. temporary passwords should be unique to an individual and should not be guessable;

Secure logon procedure

1. don't display system or application identifiers until the log-on process has been successfully completed (configurable);
2. display a general notice warning that the computer should only be accessed by authorized users (Configurable as a choice and for the message to display);
3. don't provide help messages during the log-on procedure that would aid an unauthorized user;
4. validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect;
5. limit the number of unsuccessful log-on attempts allowed, e.g. to three attempts (configurable with 0 = unlimited);
6. record unsuccessful and successful attempts;
7. force a time delay before further log-on attempts are allowed (configurable and exponential);
8. send an alarm message if the maximum number of log-on attempts is reached (configurable with email addresses);
9. display the following information on completion of a successful log-on:
    1. date and time of the previous successful log-on;
    2. details of any unsuccessful log-on attempts since the last successful log-on;
10. don't display the password being entered or consider hiding the password characters by symbols;
11. don't transmit passwords in clear text over a network.

If I'm not mistaken, the following are already integrated in Redmine from the items I listed above :

- Password policy items 1,2,3,7,8,9 and 10
- Secure logon procedure items 3,4,10 and 11

Thank you for considering these features!

Related issues:

Related to Redmine - Feature # 3096: Lock accounts after X failed attempts	**New**	**2009-04-01**
Related to Redmine - Feature # 19458: Add the ability to expire passwords aft...	**Closed**	

Related to Redmine - Feature # 4221: Force passwords to contain specified cha...	**Closed**	**2009-11-16**
Duplicated by Redmine - Feature # 12182: improvement password security for in...	**Closed**	

History

#1 - 2009-04-10 23:51 - Vidal Arpin

The following items from the password policy should read:

2. inclusion (configurable to force or not) of one or more numerical digits (configurable);
3. inclusion of special characters configuration choice (configurable to force or not);

#2 - 2011-03-23 10:50 - Toshi MARUYAMA

- Category set to Accounts / authentication

#3 - 2011-08-25 19:28 - khasha roholahi

- Assignee set to Toshi MARUYAMA

Hi,

It doesn't look like this feature has been implemented yet, it would be very useful for us as well to have what Vidal was asking for. Can someone work on this?

#4 - 2011-08-26 04:58 - Toshi MARUYAMA

- Assignee deleted (Toshi MARUYAMA)

#5 - 2011-11-30 20:07 - Robert Millan

- File cracklib.diff added

Hi,

I added cracklib support to Redmine. This doesn't address all your concerns with password policy, but at least some of them.

I figure you might find it helpful.

#6 - 2011-12-29 00:31 - Paul Liao

Hi Robert,

I've added your changes to my test redmine and I received an error when I restarted my apache

> no such file to load -- password (MissingSourceFile)
> Exception class:

My version of redmine is 1.2.3.

What exactly does your code do? Does it check the length of the password?

#7 - 2015-01-21 00:59 - @ go2null

I've created a plugin that implements Password Expiry and Lock Unused Account functionality.

It is alpha quality, so use at your own risk. Further, this is my first plugin, so even alpha is more advanced that it may be :-)

Would be great to receive pull request on GitHub.

https://github.com/go2null/redmine_account_policy

The intent is to add more functionality to implement User Account rules.
Here's a summary of the current (v2.6.0) status of the asks in the Description.

Password policy

1. use of both upper- and lower-case letters (case sensitivity);
    1. Plan to include in plugin
2. inclusion of one or more numerical digits;
    1. Plan to include in plugin
3. inclusion of special characters configuration choice;
    1. Plan to include in plugin
4. free of consecutive identical (configurable), all-numeric or all-alphabetic characters;
    1. Plan to include in plugin
5. change passwords at regular intervals (configurable) or based on the number of accesses (configurable); passwords for privileged accounts should be changed more frequently than normal passwords (configurable);
    1. *change passwords at regular intervals (configurable)* is implemented in plugin as **Password Expiry**.
6. avoid re-using or cycling old passwords (configurable);
    1. Redmine includes check against last password (i.e., prevent_reuse = 1)
    2. Plan to include in plugin
7. when users are required to maintain their own passwords, they should be provided initially with a secure temporary password;
    1. Redmine implements this as **Generate password**
8. change temporary passwords at the first log-on;
    1. Redmine implements this as **Must change password at next logon**
9. temporary passwords should be given to users in a secure manner; the use of third parties or unprotected (clear text) electronic mail messages should be avoided;
10. temporary passwords should be unique to an individual and should not be guessable;
    1. Redmine implements this as **Generate password**

Secure logon procedure

1. don't display system or application identifiers until the log-on process has been successfully completed (configurable);
    1. Already implemented in Redmine
2. display a general notice warning that the computer should only be accessed by authorized users (Configurable as a choice and for the message to display);
3. don't provide help messages during the log-on procedure that would aid an unauthorized user;
    1. Already implemented in Redmine
4. validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect;
    1. Already implemented in Redmine
5. limit the number of unsuccessful log-on attempts allowed, e.g. to three attempts (configurable with 0 = unlimited);
    1. Plan to include in plugin
6. record unsuccessful and successful attempts;
7. force a time delay before further log-on attempts are allowed (configurable and exponential);
    1. Plan to include in plugin
8. send an alarm message if the maximum number of log-on attempts is reached (configurable with email addresses);
9. display the following information on completion of a successful log-on:
    1. date and time of the previous successful log-on;

2. details of any unsuccessful log-on attempts since the last successful log-on;

10. don't display the password being entered or consider hiding the password characters by symbols;

1. Already implemented in Redmine

11. don't transmit passwords in clear text over a network.

#8 - 2015-01-21 06:46 - Mischa The Evil

- Related to Feature #3096: Lock accounts after X failed attempts added

#9 - 2015-01-21 06:47 - Mischa The Evil

- Duplicated by Feature #12182: improvement password security for internal authentication added

#10 - 2015-03-24 01:00 - Go MAEDA

- Related to Feature #19458: Add the ability to expire passwords after a configurable number of days added

#11 - 2019-04-24 04:19 - Go MAEDA

- Related to Feature #4221: Force passwords to contain specified character classes added

Files

cracklib.diff	1.46 KB	2011-11-30	Robert Millan