Redmine - Feature #37514

Storing credentials in the browser

2022-07-28 08:56 - Alberto Guerrero

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Wont fix		

Description

The Redmine tool is not properly defining the parameters of the login form, delegating the decision to store credentials in the user's browser to the user.

This possibility, while widely used for user convenience, poses a considerable risk of allowing an attacker to steal the session and credentials of any user who stores such information in the browser of a machine compromised by an attacker or credential-stealing malware.

Solution:

It should be possible to set a control from the redmine configuration to always request the username and password when logging in.

The code that is usually used to do this is to include the following line of code in the HTML file:
<INPUT TYPE="password" AUTOCOMPLETE="off">

History

#1 - 2022-08-02 14:37 - Holger Just

- Status changed from New to Closed

- Resolution set to Wont fix

To quote https://developer.mozilla.org/en-US/docs/Web/Security/Securing_your_site/Turning_off_form_autocompletion#the_autocomplete_attribute_and_login_fields:

> Modern browsers implement integrated password management: when the user enters a username and password for a site, the browser offers to remember it for the user. When the user visits the site again, the browser autofills the login fields with the stored values.
>
> Additionally, the browser enables the user to choose a master password that the browser will use to encrypt stored login details.
>
> Even without a master password, in-browser password management is generally seen as a net gain for security. Since users do not have to remember passwords that the browser stores for them, they are able to choose stronger passwords than they would otherwise.
>
> For this reason, many modern browsers do not support autocomplete="off" for login fields:
>
> - If a site sets autocomplete="off" for a <form>, and the form includes username and password input fields, then the browser still offers to remember this login, and if the user agrees, the browser will autofill those fields the next time the user visits the page.
> - If a site sets autocomplete="off" for username and password <input> fields, then the browser still offers to remember this login, and if the user agrees, the browser will autofill those fields the next time the user visits the page.
>
> This is the behavior in Firefox (since version 38), Google Chrome (since 34), and Internet Explorer (since version 11).

As such, your proposed change has no effect at all.

In any case, trying to disable the ability of password managers to remember and fill passwords and thus to force users to manually remember and enter passwords is an anti-pattern which results in reduced security overall. Accounts of users who leverage password managers (either built-in to their browser or externally, e.g. 1Password, Keepass* or similar) with a random long password are generally much safer than users who use shorter "rememberable" passwords.

Your vector of a compromised machine where malware steals credentials from a password manager is rather far-fetched. If a machine is compromised in such a way, the malware can also steal cookies of active sessions, intercept real login attempts (and thus steal the password again), and do a lot of other harm. For the user, this pretty much means game-over anyway. And there is very little we could do in this case.

Concluding:

- This is an anti-pattern which is universally discouraged.
- It doesn't work.