Old password is not maintained in the Change PW screen | Tiki Wiki CMS Groupware :: Development
Old password is not maintained in the Change PW screen

Status
Closed

Subject
Old password is not maintained in the Change PW screen

Version
2.x

Category
- Usability
- Regression

Feature
User Administration (Registration, Login & Banning)
Installer (profiles, upgrades and server-related issues)

Resolution status
Fixed or Solved

Submitted by
Rick Sapir / Tiki for Smarties

Volunteered to solve
Jean-Marc Libs

Lastmod by
Marc Laporte

Rating
(0)

Description
On a new 1.10 installation...

When logging in as the ADMIN for the first time, the Change Password Enforced page appears (requiring new admins to select a new password). The OLD PASSWORD field should be maintained (pre-filled) with the existing admins password (by default: ADMIN). This used to be the case in 1.9.

Pre-populate the OLD PASSWORD field with the user's existing password. This field should be disabled, so the user cannot change it.

Solution
Fixed.

Importance
5

Priority
25

Demonstrate Bug (Tiki 19+)
Please demonstrate your bug on show2.tiki.org

Version: trunk ▼

Demonstrate Bug (older Tiki versions)

Please demonstrate your bug on show.tikiwiki.org

Version: 18.x ▼

Ticket ID
1674

Created
Friday 04 April, 2008 13:27:20 GMT-0000
by Unknown

LastModif
Sunday 18 July, 2010 15:45:35 GMT-0000

Comments

Jean-Marc Libs 04 Apr 08 15:59 GMT-0000

This is not a regression. This is a deliberate security fix.
The way it worked before, the old password was transmitted in clear in the URL, easily available to anyone with access to web or proxy logs. It is not possible to go back to the previous code.

Jean-Marc Libs 04 Apr 08 16:24 GMT-0000

The purpose of the "old password" field is to check that the person in front of the computer knows the user's password (in this case, the user is admin, but this is the behaviour for any user who is required to change password).
If the correct old password is displayed, the whole purpose of the "old password" would be defeated.

Rick Sapir / Tiki for Smarties 04 Apr 08 19:27 GMT-0000

If I'm logged in Tiki should already know what my old password is. There's no need for me to re-enter it. (This is how 1.9.x used to work.)

If you look at the tiki-change_password.tpl, you'll see that there is an attempt to pre-populate the field: value="{$oldpass|escape}"

So obviously this was the original intent. I'm re-opening this. There was definately a change (regression) introduced here.

Jean-Marc Libs 04 Apr 08 21:35 GMT-0000

I know this is how 1.9.x used to work. This not a regression, it's security improvement, so people's passwords are not displayed in server logs. People reuse their passwords all the time. If you know their

old TW password, who knows how many of their other accounts use this same password ?

You say "If I'm logged in Tiki should already know what my old password is." but if you leave your computer unattended, people should not be able to come to the tiki-change_password.php page and see your password displayed, or change your password without knowing your password.

If you get to this page, chances are, you have just successfully typed your password. Why can't you just type it once again ?

I left the value="{$oldpass|escape}" part because it's used by the tiki-remind_password.php feature. Publishing a one-time expired automatically generated pawword is not a security risk, I figured.

Jean-Marc Libs 05 Apr 08 00:46 GMT-0000

I know this is how 1.9.x used to work. This not a regression, it's security improvement, so people's passwords are not displayed in server logs. People reuse their passwords all the time. If you know their old TW password, who knows how many of their other accounts use this same password ?

You say "If I'm logged in Tiki should already know what my old password is." but if you leave your computer unattended, people should not be able to come to the tiki-change_password.php page and see your password displayed, or change your password without knowing your password.

If you get to this page, chances are, you have just successfully typed your password. Why can't you just type it once again ?

I left the value="{$oldpass|escape}" part because it's used by the tiki-remind_password.php feature. Publishing a one-time expired automatically generated pawword is not a security risk, I figured.

Marc Laporte 05 Apr 08 22:24 GMT-0000

maybe a hash?

Attachments

filename	created	hits	comment	version	filetype

No attachments for this item

The original document is available at
https://dev.tiki.org/item1674-Old-password-is-not-maintained-in-the-Change-PW-screen