Installer destroys admin PW | Tiki Wiki CMS Groupware :: Development
Installer destroys admin PW

Status
● Open

Subject
Installer destroys admin PW

Version
18.x

Category
- Bug

Feature
Installer (profiles, upgrades and server-related issues)

Resolution status
New

Submitted by
hman

Lastmod by
hman

Rating
★★★★★ (0)

Description
When upgrading my trusty old installation of 12.14, which seemingly went through without errors, after it was completed, there is a mentioning in the installation wizard that sometimes the ability to log-in as admin might be lost.

This has struck here. Unfortunately, once you dismiss this information and proceed to log-in (with or without locking the installer) you'll never see this text (and the help offered therein) again...

After finishing the installer, I could not log-in as admin to unlock the site. And, as I wrote, the info is never shown again...

So I went to the database and I think I found the culprit.

In the table users_users I see that the record containing the admin carries a new password. According to my backup, the PW should be starting with "$1$9", but it is "$2y$10$".

According to PHP documentation the first characters before the dollar signs merely indicate the cryptographic method used for hashing. And it should be normal that from time to time PW will be re-encrypted by new methods like blowfish, or key lenghts. PHP docs even recommend automating this.

But due to the one-way nature of hashing it is impossible to re-encrypt passwords without help from the user, here the admin. The PW has to be entered fresh and then encrypted with the new method. It's impossible to decipher and re-crypt.

So if in the short time-span between the backup I drew and the run of the installer, the PW changes in the DB and changes cryptographic method, it must have been tampered with!

One more nail in Tikis coffin for me.

Importance
10 high

Easy to solve?
5

Priority
50

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
7905

Created
Sunday 31 October, 2021 23:59:24 GMT-0000
by hman

LastModif
Tuesday 02 November, 2021 11:21:51 GMT-0000

Comments

hman 01 Nov 21 00:06 GMT-0000

Setting the PW back to the value from the backup cures this, so this can be used as a workaround (but only for admins that have access to the DB and a recent backup, which the can grep and who feel comfortable fiddling with the DB itself).

Torsten Fabricius 01 Nov 21 00:52 GMT-0000

"One more nail in Tikis coffin for me. "
hman, what is the matter?

hman 01 Nov 21 09:10 GMT-0000

This is off-topic, but to answer your question: Tiki 18.8 is the worst I have ever seen (and I have had Tiki since version 1.9.2... The list of severe bugs in core functions is staggering. See my bug reports for details).

hman 01 Nov 21 09:46 GMT-0000

New finding: Another PW was touched. My user PW is now also on blowfish (as it, too, now starts with $2y$). In those minutes after making the backup, when my admin PW got defunct, I did try my user PW. Although that has no admin rights, I wanted to see whether I could "get a foot in the doorway", which of course did not work. But it could be the reason why my personal PW is the only user password on Blowfish now. I haven't tried it (I hesitate to unlock this Tiki at the moment), but it got touched.

This leads me to the thought that maybe it's not the installer after all, that is tampering with passwords, but possibly tiki-error_simple.php... tiki-error_simple.php is a risk of it's own. It can be abused to distribute defacing of one's Tiki, or worse. Like illegal content under foreign domain names! Which is why I opened up a security bug report for tiki-error_simple.php, which did not get any attention.

hman 01 Nov 21 10:23 GMT-0000

If it would turn out that tiki-error_simple.php could be the culprit, then this would make tiki-error_simple.php also a threat to the site itself, "not just" to it's reputation.

Attachments

filename	created	hits	comment	version	filetype

No attachments for this item

The original document is available at https://dev.tiki.org/item7905-Installer-destroys-admin-PW