Skye N. / March 05, 2015 12:57AM

Improving md5 password storage security

Just doing a general security audit of my phorum installations and noticed this. If I've got this wrong, please let me know.

With the general availability of md5 rainbow tables, if anyone hacked my phorum database and got the users table, it would be very easy to crack any passwords up to 9 chars in length because the passwords aren't salted.

Free rainbow tables.... [project-rainbowcrack.com]

The problem described.... [crackstation.net]

In the interesting of protecting my users and my own liability, I would like to change Phorum's password hashing algo to use the following salted hashes:

Salted Password Hashing - Doing it Right: [crackstation.net]

In order to implement this change, it looks like I would have to:

1. Increase the length of the password and password_temp columns in the users table

2. Change all password hashing calls in include/api/user.php
- phorum_api_user_save() doesn't have any hook to override the default md5() hashing
- could use user_authenticate hook to check login
- md5 for session vars is ok

~~3. Change all password hashing calls in login.php and register.php~~
- looks like these don't need to be changed, md5 for registration verify is ok

Any other places I should look?

Is password_temp used for anything other than registration email verification? I only see it being set to substr(md5(microtime()), 0, 8) so there's no danger of the unsalted password hash going over unecrypted SMTP. If so, I'm not going to bother salting it.

Thanks,
Skye

___
Skye Nott
Corvus Digital

Edited 5 time(s). Last edit at 03/05/2015 01:48AM by Skye N..

Thomas Seifert / March 05, 2015 09:57PM

Re: Improving md5 password storage security

I would just use php5.5 functions for password hashing -> [php.net] .
And I would do it simply in core with backward compatibility, send in a pull request ;).
password_temp is also used when you request a new password.

Thomas Seifert

eugenio / January 20, 2017 04:29PM
Re: Improving md5 password storage security
Hello,
any news about this topic? Phorum is still using not salted md5, right? Is there any plan to improve security or any module to implement salted password encryption without hacking the core code?

Thanks

Best,

Eugenio

Scott Finegan / January 20, 2017 07:49PM
Re: Improving md5 password storage security
[github.com]

> Quote
>
> Force password change option
>
> Start of renovation of our password system. First step: New administrator option to force a password change for individual or all users via the control center. After reload a page or after logging-in the user lands directly on the (already existing) "change password" dialog in the control center. A message in a red box says "For security reasons, you are required to change your password.". The user can only move inside the control center until he changed the password. Every other link is redirected to the change password dialog.

eugenio / January 23, 2017 11:12AM
Re: Improving md5 password storage security
Hello Scott,
thanks for your reply. I saw the change has been committed on 12 Oct 2016 so it has been included in the last version of Phorum? And what is this change supposed to do? I only see that it forces the users to change their password, but is the encryption still the same?

Thanks

Eugneio

Scott Finegan / January 26, 2017 06:37AM
Re: Improving md5 password storage security

Quote

Start of renovation of our password system.

If things go as planned, other changes will follow.

1) Since 1999, at three different Hosts my web sites have had unauthorized php code uploaded, and .htaccess files changed. Two of the compromised sites were accessed through weaknesses in the Host security (verified in host log files), the other was probably my fault. I was fortunate the unauthorized code only stole bandwidth. Had the bandwidth thieves wanted, they could easily intercept passwords, dump the database, delete the database, or its records, copy config files, etc.

2) Intercept passwords (man in the middle) can be done at the client, on the network (wired/wireless), or on the host server. For man in the middle, it doesn't really matter if you have the latest greatest encryption, or not since the hacker gets a copy of what they need. SSL also suffers from man in the middle issues [www.grc.com].

3) Password guessing (brute force). The largest issue is getting your users to use non-common or unique passwords of sufficient length. For any random account, this is the greatest weakness.

4) Publicly available lists of password hashes are unlikely to work. I watch what is used to attempt to login in the event log.

Based on my experience, once they can upload their own php files, security is breached.
Keep your backup(s) up to date, and test them on a test machine.

---

eugenio / January 26, 2017 09:31AM

Re: Improving md5 password storage security

All you said is correct, but storing passwords using a better encryption is so cheap in terms of development cost (probably a few lines of code) respect to its advantages that is the first thing I would implement.

Eugenio

Oliver Riesen-Mallmann / January 26, 2017 01:13PM

Re: Improving md5 password storage security

Hi Eugenio,

Quote

eugenio

All you said is correct, but storing passwords using a better encryption is so cheap in terms of development cost (probably a few lines of code) respect to its advantages that is the first thing I would implement.

I think it's a little bit more work for an existing software. You should also offer some kind of upgrade process...

It's not only a question of how to store the passwords. I think we need also a password policy and avoid a weak log out mechanism.

Personally I started a new job in December, so my contribution to Phorum is very small for the moment.

Any help is welcome! Start here: [github.com]

Regards
Oliver

---

eugenio / February 17, 2017 08:46PM

Re: Improving md5 password storage security

Hello all,
I am trying to figure out what to do to improve security.

Let's assume for a moment that you don't have to upgrade existing passwords.

Changes needed:

1) change password and password_temp to varchar(255) in DB

2) in users.php change:
$dbuser[$fld] = md5($dbuser[$fld]);
to:
$dbuser[$fld] = password_hash($dbuser[$fld], PASSWORD_DEFAULT);

3) in users.php substitute the two calls to phorum_db_user_check_login with something based on password_verify()

Quoting Skye,
"Is password_temp used for anything other than registration email verification? I only see it being set to substr(md5(microtime()), 0, 8) so there's no danger of the unsalted password hash going over unecrypted SMTP. If so, I'm not going to bother salting it."

and thinking about password_temp I see that it is generated by substr(md5(microtime()), 0, 8) for email verification and by phorum_gen_password() when the user requests a new password. It think that password_temp is always saved via phorum_api_user_save so it will start to be saved salted after modification 2) so no changes needed.That's all. What do you think?

The problem I see is that password_temp is always sent in clear via email when a user requests a new password, and it is not a one-time password but it can be used forever and this represents a possible security hole (no encryption in email) regardless of how the password is stored (salted or not salted).

Best,

Eugenio

Skye N. / February 17, 2017 09:48PM

Re: Improving md5 password storage security

I could be wrong but my feeling is that since you're only sending the first 8 chars of the encrypted password over email, there's little or no risk

___

Skye Nott
Corvus Digital

---

eugenio / February 18, 2017 12:07PM
Re: Improving md5 password storage security
Hello Skye,
why you say that only the first 8 characters are sent, when you request a new password the whole password in clear (NOT encrypted) is sent over email.

> Quote
> **Skye N.**
> I could be wrong but my feeling is that since you're only sending the first 8 chars of the encrypted password over email, there's little or no risk

---

Oliver Riesen-Mallmann / February 20, 2017 08:08AM
Re: Improving md5 password storage security
Hi Eugenio,

> Quote
> **eugenio**
> 1) change password and password_temp to varchar(255) in DB

Even if you don't care yet about upgrading, I prefer to use new password and password_temp columns in the database.

Regards
Oliver

Using Phorum since 7/2000: forum.langzeittest.de (actual version 5.2.23)
Modules "Made in Germany" for version 5.2: Author_as_Sender, CarCost, Close_Topic, Conceal_Message_Timestamp, Format_Email, Index_Structure, Mailing_List, Pervasive_Forum, Spritmonitor, Terms_of_Service and German_Language_Files_Package.

---

eugenio / February 20, 2017 10:59AM
Re: Improving md5 password storage security
Hi Oliver,
OK. Can you confirm the rest of the analysis is OK?

> Quote
> **Oliver Riesen-Mallmann**
> Hi Eugenio,
>
> 1) change password and password_temp to varchar(255) in DB

Even if you don't care yet about upgrading, I prefer to use new password and password_temp columns in the database.

Regards
Oliver

Skye N. / March 01, 2017 10:13PM
Re: Improving md5 password storage security
You're correct, I mis-read as I was thinking about account activation (email confirmation), not password reset.

Skye

Quote
eugenio
Hello Skye,
why you say that only the first 8 characters are sent, when you request a new password the whole password in clear (NOT encrypted) is sent over email.

I could be wrong but my feeling is that since you're only sending the first 8 chars of the encrypted password over email, there's little or no risk

___
Skye Nott
Corvus Digital

---

eugenio / March 01, 2017 10:21PM
Re: Improving md5 password storage security
@Skye: OK. Even in that case, however, I think it's not the first 8 chars of the encrypted password.

@phorum staff: I've sent an email to security@phorum.org, describing the changes I've done to implement salted storage and describing a (potential, not sure) security hole in the current Phorum code, but nobody replied. Is that email monitored?

Thomas Seifert / March 02, 2017 07:33AM
Re: Improving md5 password storage security
Yes, its monitored if the email doesn't go into the spam folder ;). digged it out now.

Thomas Seifert
Phorum Development Team / Mysnip-Solutions.de
Custom Phorum and general software development
worry-free Phorum Hosting

---

eugenio / March 02, 2017 10:05AM
Re: Improving md5 password storage security

Too bad it looked like a spammy message :)

Oliver Riesen-Mallmann / March 24, 2017 01:23PM

Re: Improving md5 password storage security

Hi Eugenio,

is it possible that you offer your changes as a pull request on github?

Regards
Oliver
