TYPO3 Core - Bug #66459

Epic # 84262 (Closed): [FEATURE] Update felogin to extbase

feuser has no validation settings on password apart of minLength

2015-04-16 19:34 - Angelo Previtali

Status:	Closed	**Start date:**	2015-04-16
Priority:	Should have	**Due date:**	
Assignee:		**% Done:**	0%
Category:	felogin	**Estimated time:**	0.00 hour
Target version:			
TYPO3 Version:	8	**Complexity:**	
PHP Version:	7.1	**Is Regression:**	No
Tags:		**Sprint Focus:**	

Description

A secure password validation should be implemented in the "reset password" form of felogin. Until now there is no possibility to force the user to set up a really secure password containing at least a number, a letter (maybe upper and/or lowercase) and special characters.

The actual version of feuser just validates the lengh of a password.

Related issues:

Related to TYPO3 Core - Feature #80792: Password strength meter for BE Login	**New**	**2017-04-10**
Related to TYPO3 Core - Feature #87726: Extend FrontendLoginController Hook t...	**Closed**	**2019-02-17**

History

#1 - 2015-04-16 20:42 - Wouter Wolters

- Status changed from New to Needs Feedback

Hi, if I'm right this is not about the core but about an 3rd party extension. The core does not check the length of the password at all. This is up the extension author to implement. Am I right?

#2 - 2015-04-16 21:02 - Angelo Previtali

Wouter Wolters wrote:

> Hi, if I'm right this is not about the core but about an 3rd party extension. The core does not check the length of the password at all. This is up the extension author to implement. Am I right?

Hi

if you set up the login page (with the username and password to fill out) as a CE with the build-in feuser extension from the TYPO3 CMS there is a checkbox in this settings for "retrieve lost password" for the user. If now you fill out the form with your e-mail address you get a mail with the link to the loginpage again (that comes from the feuser extension from the core of the TYPO3 CMS) for changing your password. This form has NO settings to force the user to set up a really secure password containing numbers, letters (maybe upper and/or lowercase) and/or special characters.

#3 - 2015-04-30 11:13 - Marc Maeder

Hi,
When reset password (Forgot Password link), felogin allows to take password like "12345678". This is very unsafe! It should also be able to adjust to use numbers, letters and/or special characters. I hope, this vulnerability can be fixed as soon as possible!

#4 - 2015-07-28 13:59 - Alexander Opitz

- Status changed from Needs Feedback to New

#5 - 2015-11-12 17:07 - Mathias Schreiber

- Target version deleted (next-patchlevel)

#6 - 2015-12-09 06:50 - Georg Ringer

- Subject changed from feuser has no validation settings on password apart the lengh to feuser has no validation settings on password apart the

length

- Description updated

#7 - 2015-12-09 06:53 - Georg Ringer

just to clarify things: there is absolutly no vulnurability in the form. the password itself might be weak but it is still saved hased and if EXT:rsaauth is used, also transferred secure!

feel free to improve your integration by e.g. using https://css-tricks.com/password-strength-meter!

#8 - 2015-12-09 08:31 - Marc Maeder

Hi,
A safe data transfer is not making secure a weak password. A system is unsafe, as long as a password like "12345678" is approved by the EXT:felogin.

#9 - 2015-12-12 21:51 - Georg Ringer

absolutly true. it would be great to have a password strength check everywhere where a password is set!

#10 - 2017-04-10 23:12 - Riccardo De Contardi

- Related to Feature #80792: Password strength meter for BE Login added

#11 - 2017-05-24 10:48 - DANIEL Rémy

Hello

It would be a good starting point to just have a hook that allow integrator to implement any password strength validator [1].
Actually, a hook exists, but just for the password hashing mecanism (used by ext:saltedpasswords).

If the core team are OK, I can push some code to start working on this.

[1] A password strength library by Dropbox: https://github.com/dropbox/zxcvbn

#12 - 2017-09-08 16:12 - Marc Maeder

- TYPO3 Version changed from 6.2 to 8

- PHP Version changed from 5.5 to 7.1

Why is a secure password validation in "reset password" still not implemented in Typo3 V8? Will this be realized in the next weeks?

#13 - 2017-10-19 15:37 - Marc Maeder

Hi,
A Workaround to make a secure password validation in EXT:felogin. The disadvantage is that it is overwritten with the core update!

ext_localconf.php (2 adjustments)
Line 57: Set newPasswordMinLength to 8 or a higher value (instead of 6)
After line 141 insert this new line for a new message:
changePasswordMissingCharsMessage_stdWrap < .welcomeMessage_stdWrap

Classes/Controller/FrontendLoginController.php (2 adjustments)
Line 308: $minLength = (int)$this->conf['newPasswordMinLength'] ?: 8; (or a higher value, instead of 6)
After line 347 insert this new lines for the the new validation of missing chars:
} elseif (preg_match("#^[a-zA-Z0-9]+$#",$postData['password1'])) {
$markerArray['###STATUS_MESSAGE###'] = sprintf($this->getDisplayText(
'change_password_missingchars_message',
$this->conf['changePasswordMissingCharsMessage_stdWrap.']),
$minLength
);

Ressources/Private/Language/locallang.xlf (1 adjustment)
After line 79 insert this new lines for the the new message:
<trans-unit id="ll_change_password_missingchars_message">
<source>The password is not secure. Please enter your new password twice. Password needs a minimum length of %s chars and at least letters, numbers and special characters.</source>
</trans-unit>

typo3conf/l10n/de/felogin/Ressources/Private/Language/de.locallang.xlf (or path to file of any other languages with the corresponding translation)
After line 41 insert this new lines for the the translation of the new message (e.g. in german file):
<trans-unit id="ll_change_password_missingchars_message" approved="yes">
<source>The password is not secure! Please enter your new password twice. Password needs a minimum length of %s chars and at least letters, numbers and special characters.</source>

<target state="translated">Das Passwort ist nicht sicher! Das neue Passwort bitte zweimal eingeben. Es ist eine Mindestlänge von %s Zeichen erforderlich und es muss aus Buchstaben, Zahlen und Sonderzeichen bestehen.</target>
</trans-unit>

#14 - 2019-04-10 11:59 - Stephan Großberndt

- Subject changed from feuser has no validation settings on password apart the length to feuser has no validation settings on password apart of minLength

- Status changed from New to Resolved

The patch

https://github.com/TYPO3/TYPO3.CMS/commit/39441104649280393f3c54a5bb33b67be294f41a
'Added feature #10017: [felogin] New Method for "forgotPassword"'

added a hook to pass the password to an extension implementing that hook in 2009, available since TYPO3 4.3.

Back then it was not possible to stop the password from being saved if the hook finds it unsuitable apart from die() in the hook.
Only recently this was improved: From TYPO3 v10 on you do not have to resort changing TYPO3 core code as

https://forge.typo3.org/issues/87726
https://review.typo3.org/c/Packages/TYPO3.CMS/+/59714

added such a validation possibility.

#15 - 2019-04-10 12:01 - Stephan Großberndt

- Status changed from Resolved to New

Still this should be considered a missing TYPO3 core feature.

#16 - 2019-04-10 12:01 - Stephan Großberndt

- Related to Feature #87726: Extend FrontendLoginController Hook to validate password added

#17 - 2019-04-10 12:23 - Stephan Großberndt

- Parent task set to #84262

#18 - 2020-03-08 20:40 - Benni Mack

- Status changed from New to Closed

I agree, this can now be fully configured in TYPO3 v10 with any kind of Extbase Validators. I will close this issue for the time being - if you feel we should continue working on this, let me know, so I can re-open the issue - or just open a new ticket with the specifics that you still miss with TYPO3 v10.