

TYPO3.Flow - Bug # 32991

Status:	Resolved	Priority:	Should have
Author:	Karsten Dambekalns	Category:	Security
Created:	2012-01-05	Assigned To:	Karsten Dambekalns
Updated:	2012-05-04	Due date:	
PHP Version:			
Has patch:	No		
Complexity:			
Affected Flow version: Git master			
Subject:	Wrong default password hashing strategy		
Description			
In https://review.typo3.org/5756 the default hashing strategy was changed to BCrypt.			
Later, in https://review.typo3.org/6598 , support for multiple strategies was added. But that change make PBKDF2 the default again.			
Related issues:			
related to TYPO3.Flow - Feature # 31678: Support BCrypt (Blowfish crypt) pass...		Resolved	2011-11-08
related to TYPO3.Flow - Feature # 31679: Support multiple password hashing st...		Resolved	2011-11-08

Associated revisions

Revision 28a049fc - 2012-04-26 13:28 - Karsten Dambekalns

[BUGFIX] Make BCrypt the default hashing strategy (again)

In <https://review.typo3.org/5756> the default hashing strategy was changed to BCrypt. Later, in <https://review.typo3.org/6598>, support for multiple strategies was added. But that change make PBKDF2 the default again.

This change fixes that and makes the SaltedMd5 strategy available in the YAML file as well (for completeness).

Change-Id: Icb1886a63031ae8393c391a99f7616cfb0a35b96

Fixes: #32991

Releases: 1.1

Revision 78279ca9 - 2012-04-27 17:02 - Christopher Hlubek

[BUGFIX] Implement fallback for password hash migration

The new BCrypt default hashing strategy causes problems if a FLOW3 application is migrated from version 1.0 which didn't use strategy identifiers inside credentials. A new "fallback" configuration option allows to specify the strategy that was used to generate these legacy credentials. It defaults to "pbkdf2" and allows for a seamless migration from 1.0 to 1.1. New passwords will be hashed with the default strategy ("bcrypt" by default) and get the strategy identifier prepended.

Change-Id: Ib817adb43552abfccc587bbbe5e1f55fd860a39c

Fixes: #32991

Releases: 1.1

History

#1 - 2012-01-05 11:50 - Gerrit Code Review

- *Status changed from New to Under Review*

Patch set 1 for branch **master** has been pushed to the review server.

It is available at <http://review.typo3.org/7681>

#2 - 2012-01-05 12:07 - Karsten Dambekalns

- *Assigned To set to Karsten Dambekalns*

#3 - 2012-04-26 13:28 - Gerrit Code Review

Patch set 2 for branch **master** has been pushed to the review server.

It is available at <http://review.typo3.org/7681>

#4 - 2012-04-26 14:38 - Karsten Dambekalns

- *Status changed from Under Review to Resolved*

- *% Done changed from 0 to 100*

Applied in changeset commit:28a049fc0d5ca17e5ee1ec8c92c020aa9a32864c.

#5 - 2012-04-27 17:02 - Gerrit Code Review

- *Status changed from Resolved to Under Review*

Patch set 1 for branch **master** has been pushed to the review server.

It is available at <http://review.typo3.org/10832>

#6 - 2012-05-04 02:38 - Christopher Hlubek

- *Status changed from Under Review to Resolved*

Applied in changeset commit:78279ca9a0c1b6808db415b678722791c66f4d0f.