TYPO3.Flow - Bug # 47725

Status:	Resolved	**Priority:**	Could have
Author:	Christopher Hlubek	**Category:**	Security
Created:	2013-04-30	**Assigned To:**	Christopher Hlubek
Updated:	2014-07-11	**Due date:**	
PHP Version:			
Has patch:	No		
Complexity:			
Affected Flow version:	Git master		
Subject:	BCrypt hashing should support migration of older costs		

Description

In the current implementation of the BCryptHashingStrategy a password is hashed with crypt and the hash contains the algorithm and parameters with the salt that was used to hash the password.

During validation only the salt is taken from the hashed password, so the cost parameter has to match the original cost. This is very problematic if the cost needs to be changed during the lifetime of a project. A high cost means slow logins but more securely hashed passwords.

The hashing strategy should be able to validate an existing hash with a different cost for migration of password hashes and updates to the cost parameter during the lifetime of a project (with hardware improvements the hashing will always get cheaper during time).

Associated revisions

Revision 8872a65b - 2013-04-30 11:27 - Christopher Hlubek

[BUGFIX] Support BCrypt validation of hashes with different cost

In the current implementation of the BCryptHashingStrategy a password is hashed with crypt and the hash contains the algorithm and parameters with the salt that was used to hash the password.

This change updates the validation to also take the cost from the stored hash and allow changes to the cost setting.

Change-Id: I7dcc1425c06e3e542b545fad367a1d91d6a65689
Fixes: #47725
Releases: master, 2.0

Revision 269b2582 - 2014-01-31 15:40 - Christopher Hlubek

[BUGFIX] Support BCrypt validation of hashes with different cost

In the current implementation of the BCryptHashingStrategy a password is hashed with crypt and the hash contains the algorithm and parameters with the salt that was used to hash the password.

This change updates the validation to also take the cost from the stored hash and allow changes to the cost setting.

Change-Id: I7dcc1425c06e3e542b545fad367a1d91d6a65689

Fixes: #47725

Releases: master, 2.0

History

#1 - 2013-04-30 11:27 - 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 https://review.typo3.org/20349

#2 - 2013-05-21 12:17 - Robert Lemke

- Priority changed from Should have to Could have

- Target version set to 2.0

#3 - 2013-08-14 15:35 - Karsten Dambekalns

- Target version changed from 2.0 to 2.0.1

#4 - 2014-01-31 15:40 - Gerrit Code Review

Patch set 1 for branch **2.0** of project **Packages/TYPO3.Flow** has been pushed to the review server.

It is available at https://review.typo3.org/27199

#5 - 2014-07-11 20:19 - Christopher Hlubek

- Status changed from Under Review to Resolved

- % Done changed from 0 to 100

Applied in changeset commit:8872a65bc437cd3d1d2275b9657ceb92ad19e492.