TYPO3 Flow Base Distribution - Feature #26786

Use a safe password hashing mechanism

2011-05-12 16:36 - Christopher Hlubek

Status:	Resolved	**Start date:**	2011-05-12
Priority:	Must have	**Due date:**	
Assignee:	Christopher Hlubek	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	1.0 beta 1		

Description

The current AccountFactory uses the generateSaltedMd5 method of the HashService. Since MD5 is considered to be not safe, we should switch to either sha1 or another method for password hashing (e.g. also use an hmac).

Related issues:

Related to TYPO3 Core - Feature #28230: Add support for PBKDF2 to hashing	**Closed**	**2011-07-15**

Associated revisions

Revision ad4c9a7e - 2011-07-15 12:46 - Christopher Hlubek

[!!!][FEATURE] Implement a safe password hashing mechanism using PBKDF2

This change implements a configurable password hashing strategy for
the hash service and a PBKDF2 based password hashing strategy which
generates strong hashed passwords and uses multiple iterations for
brute-force protection.

To use the old salted MD5 hashing, the password hashing strategy
may be replaced in the Objects.yaml.

Change-Id: I9d365a9eab3930433f49faf9e7c8c5fbb1166dcc
Resolves: #26786

History

#1 - 2011-05-19 12:35 - Christopher Hlubek

I would suppose to use a standardized and proven way of creating password hashes for storage: see http://en.wikipedia.org/wiki/PBKDF2 and http://www.itnewb.com/v/Encrypting-Passwords-with-PHP-for-Storage-Using-the-RSA-PBKDF2-Standard

With a decent iteration count (> 10,000) it should be considered safe for now.

#2 - 2011-05-24 12:00 - Mr. Hudson

Patch set 1 of change I9d365a9eab3930433f49faf9e7c8c5fbb1166dcc has been pushed to the review server.
It is available at http://review.typo3.org/2332

#3 - 2011-05-24 12:20 - Mr. Hudson

Patch set 2 of change I9d365a9eab3930433f49faf9e7c8c5fbb1166dcc has been pushed to the review server.
It is available at http://review.typo3.org/2332

#4 - 2011-05-24 12:40 - Christopher Hlubek

- Status changed from New to Under Review

- Assignee set to Christopher Hlubek

I implemented a PBKDF2 based password hashing and refactored the hash service to enable configurable password hashing strategies.

#5 - 2011-05-27 10:52 - Mr. Hudson

Patch set 4 of change I9d365a9eab3930433f49faf9e7c8c5fbb1166dcc has been pushed to the review server.
It is available at http://review.typo3.org/2332

#6 - 2011-07-15 12:27 - Mr. Hudson

Patch set 5 of change I9d365a9eab3930433f49faf9e7c8c5fbb1166dcc has been pushed to the review server.
It is available at http://review.typo3.org/2332

#7 - 2011-07-15 12:47 - Mr. Hudson

Patch set 6 of change I9d365a9eab3930433f49faf9e7c8c5fbb1166dcc has been pushed to the review server.
It is available at http://review.typo3.org/2332

#8 - 2011-07-18 12:05 - Christopher Hlubek

- Status changed from Under Review to Resolved

- % Done changed from 0 to 100

Applied in changeset commit:ad4c9a7e4e6950c16c4a2cf138bafe69958af8ca.