TYPO3.Flow - Bug # 28257

Status:	Resolved	**Priority:**	Should have
Author:	Bastian Waidelich	**Category:**	Security
Created:	2011-07-16	**Assigned To:**	Karsten Dambekalns
Updated:	2011-08-26	**Due date:**	
PHP Version:			
Has patch:			
Complexity:			
Affected Flow version:			
Subject:	Avoid Credentials to be stored in the request		

Description

When you authenticate using the PersistedUsernamePasswordProvider username & password are copied to the **GET Arguments** of the following request when used in SubRequests (plugins / widgets) because POST arguments are merged in the RequestBuilder. To avoid this, we should use "internal request arguments" for authentication (see #25802).

Concrete: The strings 'TYPO3.FLOW3.Security.Authentication.Token.UsernamePassword.username' and 'TYPO3.FLOW3.Security.Authentication.Token.UsernamePassword.password' in \TYPO3\FLOW3\Security\Authentication\Token\UsernamePassword::updateCredentials() should be replaced.
It could even be just __username & __password IMO.

Note: documentation and referring comments needs to be adjusted. To avoid headache, the token could still check for the old post vars and throw an exception (in dev context) / create a log entry (in other contexts)

Associated revisions

Revision c78ca09b - 2011-08-25 17:44 - Bastian Waidelich

[!!!][BUGFIX] Avoid Credentials to be stored in the request

When you authenticate using the PersistedUsernamePasswordProvider username & password are copied to the GET Arguments of the following request when used in SubRequests (plugins / widgets) because POST arguments are merged in the RequestBuilder.

This change fixes this by prepending username & password with two underscores, turning them into "internal request arguments" (see #25802)

Change-Id: Ifdee053fc1c1dc2338dddf7b759ce6b6bcd00a26
Resolves: #28257

History

#1 - 2011-07-16 17:20 - Mr. Hudson

- Status changed from New to Under Review

Patch set 1 of change Ifdee053fc1c1dc2338dddf7b759ce6b6bcd00a26 has been pushed to the review server.
It is available at http://review.typo3.org/3375

#2 - 2011-07-16 17:22 - Mr. Hudson

Patch set 2 of change Ifdee053fc1c1dc2338dddf7b759ce6b6bcd00a26 has been pushed to the review server.
It is available at http://review.typo3.org/3375

#3 - 2011-08-16 10:40 - Karsten Dambekalns

Well, about the simple rename - we support multiple tokens and all that fuzz. So, wouldn't we need to be able to separate login data for different tokens / providers? Andreas, what do you think?

#4 - 2011-08-24 12:38 - Bastian Waidelich

Karsten Dambekalns wrote:

> *Well, about the simple rename - we support multiple tokens and all that fuzz. [...]*

Not sure.. but we could replace
1<inputtype="text"name="TYPO3[FLOW3][Security][Authentication][Token][UsernamePassword][username]".../>
with
1<inputtype="text"name="__authentication[TYPO3.FLOW3][Security][Authentication][Token][UsernamePassword][username]".../>

to make sure..

#5 - 2011-08-25 11:14 - Karsten Dambekalns

- Status changed from Under Review to Accepted
- Assigned To set to Karsten Dambekalns

I'll adjust the change.

#6 - 2011-08-25 12:45 - Mr. Hudson

- Status changed from Accepted to Under Review

Patch set 3 of change Ifdee053fc1c1dc2338dddf7b759ce6b6bcd00a26 has been pushed to the review server.
It is available at http://review.typo3.org/3375

#7 - 2011-08-25 13:34 - Mr. Hudson

Patch set 4 of change Ifdee053fc1c1dc2338dddf7b759ce6b6bcd00a26 has been pushed to the review server.
It is available at http://review.typo3.org/3375

#8 - 2011-08-25 17:45 - Mr. Hudson

Patch set 5 of change Ifdee053fc1c1dc2338dddf7b759ce6b6bcd00a26 has been pushed to the review server.
It is available at http://review.typo3.org/3375

#9 - 2011-08-26 09:36 - Bastian Waidelich

- Status changed from Under Review to Resolved

- % Done changed from 0 to 100

Applied in changeset commit:c78ca09b43614a84601f2f121c9f1c68bcb89350.