TYPO3.Flow - Bug # 25859

Status:	Resolved	**Priority:**	Must have
Author:	Bastian Waidelich	**Category:**	Security
Created:	2011-04-08	**Assigned To:**	Andreas Förthner
Updated:	2011-04-14	**Due date:**	

PHP Version:	
Has patch:	
Complexity:	
Affected Flow version:	
Subject:	CSRF protection does not work for methods that contain upper case characters

Description

I'm trying to protect all methods of certain controllers with following policy rule:

    resources:
     methods:
      F3_BccVoting_RestrictedControllers: 'class(F3\BccVoting\Controller\(Circular|Elector|Electorate)Controller)'

For some reason the FLOW3-CSRF-TOKEN is not attached to links pointing to F3\BccVoting\Controller\Elector::deleteAll(). When clicking the link, the "You are not allowed to perform this action." exception though.

The problem is probably, that the policy service does not detect the method in the CsrfProtectionAspect because it is lowercased somewhere.

Associated revisions

Revision 797fcc64 - 2011-04-14 16:31 - Bastian Waidelich

[+BUGFIX] Fix CSRF protection for camelCased actions

The FLOW3-CSRF-TOKEN is not attached to links pointing to
actions that contain upper case letters.
The solution is to store and compare all resources lowercased.

Change-Id: Ibae8ad81a7839c983b64bad86a8631c0176c59b1
Fixes: #25859

History

#1 - 2011-04-08 17:44 - Andreas Förthner

solution: all methods and classes should be stored and checked in lowercase in the security context...

#2 - 2011-04-11 10:19 - Mr. Hudson

Patch set 1 of change Ibae8ad81a7839c983b64bad86a8631c0176c59b1 has been pushed to the review server.
It is available at http://review.typo3.org/1543

#3 - 2011-04-14 16:22 - Mr. Hudson

Patch set 2 of change Ibae8ad81a7839c983b64bad86a8631c0176c59b1 has been pushed to the review server.

It is available at http://review.typo3.org/1543

#4 - 2011-04-14 16:31 - Mr. Hudson

Patch set 3 of change Ibae8ad81a7839c983b64bad86a8631c0176c59b1 has been pushed to the review server.

It is available at http://review.typo3.org/1543

#5 - 2011-04-14 17:30 - Bastian Waidelich

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset commit:797fcc64b3a491861b7bdc0b732788a66229cd55.