TYPO3.Flow - Bug # 36776

Status:	Resolved	**Priority:**	Should have
Author:	Sebastian Kurfuerst	**Category:**	MVC
Created:	2012-05-02	**Assigned To:**	Sebastian Kurfuerst
Updated:	2012-05-15	**Due date:**	
PHP Version:			
Has patch:	No		
Complexity:			
Affected Flow version:	Git master		
Subject:	Property Mapping should be based on whitelist; configuration should be generated by form		

Description

In order to make the property mapper more predictible and secure by default, we propose the following changes:

- We should be able to **explicitely** map allowed fields, and ignore all non-specified fields.
- If passing an object inside a link f.e., no modification of this object should be allowed at all
- if using Fluid, it should be safe by default but not required to specify any property mapping configuration

Following are the changes needed:

Change PropertyMappingConfiguration
!!! BREAKING PropertyMappingConfiguration::shouldMap() should use WHITELIST instead of BLACKLIST

- if a property is on blacklist, return FALSE directly
- if a property is on whitelist, return TRUE
- if all property are on whitelist, return TRUE
- by default, return FALSE

- $cfg->forProperty('image.author')->allowProperties('foo', 'bar')
- $cfg->forProperty('image.author')->allowAllProperties()
- $cfg->forProperty('image.author')->allowAllPropertiesExcept('foo')

- Usually, you only use one of the following, not all of them!

PropertyMappingConfigurationBuilder should not set any type converter options by default

- !!! BREAKING PropertyMappingConfigurationBuilder should NOT set any type converter options by default, especially not CONFIGURATION_CREATION_ALLOWED or CONFIGURATION_MODIFICATION_ALLOWED

generation of HMAC in Fluid Form Fields

!!! Fluid Form Fields should generate Property Mapping configuration of allowed fields appropriately
-> similar to v4 processRequest

Adjust ActionController

Action Controller: PropertyMapping config should be set from HMAC.

5) DOCUMENTATION:
wenn man nur bestimmte Objekte editieren soll (bspw. alle Blogs mit geradem erstellungsdatum) --> POLICY!!
--> values protected? (e.g. hidden fields / identity values that can't be changed)

Associated revisions

Revision 3f6576e4 - 2012-05-15 12:57 - Sebastian Kurfuerst

[!!!][FEATURE] (MVC): Whitelist-based Property Mapping Configuration

Up to now, property mapping always allowed to modify all properties of a given
object. Especially in the MVC stack, this functionality was relied upon for
all update and create actions. However, for nested objects, the user needed
to configure whether updates and creations should be allowed.

This was an inconsistent behavior, especially because for read-only actions the
object could be also modified.

The behavior is now changed to be more predictive:

- the default PropertyMappingConfiguration used in the MVC stack is changed
  to be very restrictive: we do neither allow creation of any new objects nor
  modification of existing ones; and all properties which should be modified
  must be explicitly configured.

- For each form, Fluid now generates a list of trusted properties, based upon
  which the PropertyMappingConfiguration is set correctly. This means only
  properties which have been rendered by fluid are allowed to be modified,
  and creation / insertion is only permitted if needed.

BREAKING CHANGES

- PropertyMappingConfiguration::doNotMapProperty (no public API) was removed.
  Instead, use ::allowAllPropertiesExcept(…).
- Furthermore, an exception is now thrown if a property is not allowed to be
  mapped. Before, the property was just ignored silently. You should either
  write your own TypeConverter to deal with that or filter the input data
  correctly before property mapping.

In a nutshell:

- If you used Fluid forms, everything will still work as expected.
- If you used Fluid forms and needed to adjust the property mapping configuration
  manually, you can remove these manual adjustments.
- If you manually called the Property Mapper and passed a custom Property Mapping
  Configuration, you probably need to call …->allowAllProperties() on the property
  mapping configuration.
- If you did not used Fluid forms but relied upon the old behavior of the Property
  Mapper (e.g. in a web service), you need to configure the Property Mapper
  inside your initializeAction correctly now.

Note: You need the accompanying Fluid change for testing this feature as well.

Change-Id: Iac7bbb2a58ad890701fff2b0ad6b16a0e0b15bba
Resolves: #36776
Releases: 1.1

Revision 18e7219f - 2012-05-15 12:57 - Sebastian Kurfuerst

[FEATURE] Inclusion of DomCrawler in Functional Test Browser

In order to run meaningful end-to-end functional tests, we need a way
to navigate through HTML by clicking links and submitting forms.

We use DomCrawler to make this possible. This needs to be included
separately.

Change-Id: I44d69f108fe91625f52817e538216e736d30659b
Related: #36776
Resolves: #36830
Releases: 1.1

Revision 94d958a5 - 2012-05-29 10:17 - Bastian Waidelich

[BUGFIX] Set property mapping configuration in RestController

Since Iac7bbb2a58ad890701fff2b0ad6b16a0e0b15bba we use a
whitelist-based approach to configure property mapping.
This change hooks into the create/update action of the
RestController and sets the required property mapping
configuration.

Change-Id: I6edbef57b42ed7afa176fbe231c500ff5fec8b14
Related: #37402
Related: #36776
Releases: 1.1, 1.2

History

#1 - 2012-05-02 14:44 - Gerrit Code Review

- Status changed from Accepted to Under Review

Patch set 1 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/10926

#2 - 2012-05-02 16:24 - Gerrit Code Review

Patch set 2 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/10926

#3 - 2012-05-02 16:41 - Gerrit Code Review

Patch set 3 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/10926

#4 - 2012-05-02 16:45 - Gerrit Code Review

Patch set 4 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/10926

#5 - 2012-05-04 07:52 - Gerrit Code Review

Patch set 5 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/10926

#6 - 2012-05-04 22:54 - Helmut Hummel

This is something that needs to be changed in extbase as well, right? Is there already an accompanying ticket in the extbase tracker?

#7 - 2012-05-15 10:05 - Gerrit Code Review

Patch set 6 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/10926

#8 - 2012-05-15 12:57 - Gerrit Code Review

Patch set 7 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/10926

#9 - 2012-05-15 14:38 - Sebastian Kurfuerst

- Status changed from Under Review to Resolved
- % Done changed from 0 to 100

Applied in changeset commit:3f6576e47756a170d98232ff7f5a35d679052701.