TYPO3.Fluid - Bug # 5256

Status:	Resolved	**Priority:**	Should have
Author:	Karsten Dambekalns	**Category:**	Core
Created:	2009-11-06	**Assigned To:**	Karsten Dambekalns
Updated:	2010-10-20	**Due date:**	
Has patch:			
Affected Flow version:			
Subject:	htmlspecialchars() applied inconsistently and of little use		

Description

Observations:

- When a value assigned to Fluid is put into a template, it remains untouched (i.e. angle brackets stay as they are and so forth).
- When a value is passed through a ViewHelper, it is by default run through HtmlSpecialCharsPostProcessor
  - This can be disabled only by using a setting that is not part of the public API and subject to change

So, the processing of values is not consistent. But there is more:

I would expect to be able to use the values assigned as-is, unprocessed. An example are the templates used in the FLOW3 kickstarter, where angle brackets are completely legal and must not be run through htmlspecialchars().
Therefore I propose the following:

- remove the HtmlSpecialCharsPostProcessor (and possible the whole ObjectAccessorPostProcessorInterface and related code)
- add a ViewHelper that can be used with inline syntax to apply escaping for HTML (e.g. like {value->f:escapeForHtml})

That way the user can decide how to make use of the values.

Related issues:

related to TYPO3.Fluid - Feature # 5257: Allow generic post-processing of tem...	**Resolved**	**2009-11-06**

History

#1 - 2009-11-06 16:37 - Bastian Waidelich

- Category set to Core

As a reminder:

1. Object accessor nodes (e.g. {customer.name})should be processed by the ObjectAccessorPostProcessor too of course. If that's not the case, that's a bug

2. The original plan was to make post processors configurable per template & package. But IMHO we should keep the HtmlSpecialCharsPostProcessor by default - at least for HTML templates. Otherwise there would be no easy way to protect yourself from XSS attacks

#2 - 2009-11-09 12:11 - Karsten Dambekalns

Bastian Waidelich wrote:

> *1. Object accessor nodes (e.g. {customer.name})should be processed by the ObjectAccessorPostProcessor too of course. If that's not the case, that's a bug*

That was indeed a bug and has been fixed by Sebastian in r3461.

#3 - 2009-11-23 15:50 - Karsten Dambekalns

- Status changed from Accepted to Resolved

- % Done changed from 0 to 100

The bug contained here has been fixed, the remaining stuff has it's own issue.