TYPO3.Flow - Bug # 2851

Status:	Resolved	**Priority:**	Must have
Author:	Jochen Rau	**Category:**	Validation
Created:	2009-03-16	**Assigned To:**	Andreas Förthner
Updated:	2010-10-20	**Due date:**	
PHP Version:			
Has patch:			
Complexity:			
Affected Flow version:			
Subject:	TextValidator is insecure		

Description

The TextValidator is insecure. It filters an input string based on a black list only with ASCII chars:

```
if (!is_string($value) || preg_match('/<[\/]*[a-z,A-Z,0-9]*>/', $value)) {
[...]
}
```

XSS injections could be decoded e.g. in hexadecimal format. I propose the following solution:

```
if ($value !== filter_var($value, FILTER_SANITIZE_STRING)) {
[...]
}
```

-- jochen

Related issues:

related to TYPO3.Flow - Bug # 3977: TextValidator is insecure	**Rejected**

Associated revisions

Revision 9f5ed7f9 - 2009-03-26 23:55 - Karsten Dambekalns

FLOW3:

- TextValidator now uses filter_var() to check value, refs #2851

History

#1 - 2009-03-26 23:36 - Karsten Dambekalns

- Status changed from New to Accepted

- Assigned To changed from Andreas Förthner to Karsten Dambekalns

Won by Jochen Weiland during the bug auction at T3BOARD09

#2 - 2009-03-26 23:55 - Karsten Dambekalns

- Assigned To changed from Karsten Dambekalns to Andreas Förthner

#3 - 2009-03-27 00:25 - Andreas Förthner

- Status changed from Accepted to Resolved

I could not find any other XSS strings, as they all need some kind of HTML-Tag in the string. Encoded tags are already sanitized.

Files

TextValidator.diff	577 Bytes	2009-03-16	Jochen Rau