TYPO3.Flow - Task # 7031

Status:	Resolved	**Priority:**	Must have
Author:	Marcus Krause	**Category:**	Security
Created:	2010-03-27	**Assigned To:**	Karsten Dambekalns
Updated:	2010-10-20	**Due date:**	
Sprint:			
PHP Version:			
Has patch:			
Complexity:			
Subject:	Unsafe masking of a dynamic regex pattern		

Description

F3\FLOW3\Security\RequestPattern\Uri has method matchRequest() that uses a dynamic regex pattern.

```
return (boolean)preg_match('/^' . str_replace('/', '\/', $this->uriPattern) . '$/', $request->getRequestUri()->getPath());
```

Masking is done by str_replace(). This is not sufficient; think of a pattern that contains with '\/'. There's a dedicated method preq_quote() that takes care of proper masking.

So masking itself should be

```
preg_quote($this->uriPattern, '/')
```

Please grep through the complete code to possibly find similiar code; I haven't done that (I am using forge repository interface right now).

Associated revisions

Revision 9ad22f0f - 2010-04-15 18:26 - Karsten Dambekalns

[~TASK] FLOW3 (Security): Clarified what happens to the pattern in RequestPattern\Uri, resolves #7031.

History

#1 - 2010-04-07 12:18 - Karsten Dambekalns

- Category set to Security

- Status changed from New to Needs Feedback

- Assigned To set to Karsten Dambekalns

- Start date deleted (2010-03-27)

- Estimated time set to 1.00

Well, preg_quote() masks all characters that have a meaning in a regex. This is not wanted in this case, at least judging from the doc comments the pattern can be a full-fledged regex. Running that through preg_quote() would render it useless.

The question remains, whether the str_replace() is really helpful here. Either way the documentation needs to instruct the user on what happens to the pattern, so the right stuff can be fed into the class.

#2 - 2010-04-07 16:14 - Andreas Förthner

yes, I'm all for leaving it as a real regex configuration option. But you are right that the current situation is somehow inconsistent. On the other hand it's just convenient not to have to escape slashes in a URI pattern. What do you think, should we just add a note to the documentation that slashes will be automatically escaped? Or should we drop this automatic escaping and make a real regex pattern out of this option?

#3 - 2010-04-07 18:25 - Karsten Dambekalns

I am for leaving it like it is, but making clear what happens in the documentation.

#4 - 2010-04-15 17:50 - Karsten Dambekalns

- Due date set to 2010-04-15
- Target version set to 1.0 alpha 8

#5 - 2010-04-15 17:51 - Karsten Dambekalns

- Due date deleted (2010-04-15)
- Start date set to 2010-04-15

#6 - 2010-04-15 18:24 - Karsten Dambekalns

- Tracker changed from Bug to Task

#7 - 2010-04-15 18:27 - Karsten Dambekalns

- Status changed from Needs Feedback to Accepted

#8 - 2010-04-15 19:00 - Karsten Dambekalns

- Status changed from Accepted to Resolved
- % Done changed from 0 to 100

Applied in changeset r4155.