

TYPO3.Flow - Feature # 6604

Status:	Resolved	Priority:	Must have
Author:	Andreas Förthner	Category:	Security
Created:	2010-02-25	Assigned To:	Andreas Förthner
Updated:	2010-10-20	Due date:	
PHP Version:			
Has patch:			
Complexity:			
Subject:	Implement QueryRewriting according to the security policy		
Description			
<p>Queries to the persistence layer should be automatically rewritten according to the security policy. This will speed up things a lot, as you'll only get objects you'll actually be allowed to see.</p> <p>One idea was to define constraints for models in the Policy.yaml:</p> <pre>resources: models: F3\Party\Domain\Model\Account: ownAccount: this.party == current.party && this.credentialsSourec != 'foo'</pre> <p>Another idea came to my mind, that we should discuss:</p> <p>Often you want to define access for specific models on a per object basis. Meaning you want to define which roles should be allowed to see a specific object. This ends up in adding roles to objects, which we could do by a cool model security advice. We'll have to discuss this in details!</p>			
Related issues:			
related to TYPO3.Flow - Major Feature # 5659: Implement content security		Resolved	2009-12-07

Associated revisions

Revision 23ce4758 - 2010-06-23 14:31 - Andreas Förthner

- [+TASK] FLOW3 (Object): Added session scope related methods to the object manager and interface.
- [+FEATURE] FLOW3 (AOP): Added a matches operator as a new possibility for runtime evaluations.
- [+FEATURE] FLOW3 (AOP): Global objects available in runtime evaluations can now be configured in the settings. Resolves #6598.
- [+FEATURE] FLOW3 (Security): Implemented query rewriting according to the security policy. Relates to #5659, Resolves #6604.

Revision 8740afe8 - 2010-06-25 16:02 - Karsten Dambekalns

[~TASK] FLOW3 (Persistence): If objects have been blocked by security query rewriting, ignore them in certain places; relates to #6604.

Revision 92e5324c - 2010-06-27 21:20 - Karsten Dambekalns

[~TASK] FLOW3 (Persistence): Adjusted unit tests not included in last commit (If objects have been blocked by security query rewriting, ignore them in certain places); relates to #6604.

History

#1 - 2010-03-02 17:12 - Andreas Förthner

- Target version set to 1.0 alpha 9

#2 - 2010-03-02 17:13 - Andreas Förthner

- Priority changed from Should have to Must have

#3 - 2010-03-03 22:09 - Andreas Förthner

We have to advice three methods of the Persistence BackendInterface:

getObjectCountByQuery(\$query):

-> rewrite QOM \$query by setting appropriate constraints as where conditions for top level objects, or join conditions for subobjects

getObjectDataByQuery(\$query):

-> rewrite QOM \$query by setting appropriate constraints as where conditions for top level objects, or join conditions for subobjects

getObjectDataByIdentifier(\$identifier):

-> check the return value (this is always only one object)

#4 - 2010-03-03 22:14 - Andreas Förthner

In the policy we need to following comparison operators:

==

>=

<=

>

<

!=

like

<arrayProperty> contains <singleValue>

<singleValueProperty> in <array of values>

<arrayProperty> matches <array of values>

#5 - 2010-03-11 10:54 - Robert Lemke

- Start date changed from 2010-02-25 to 2010-03-04

- % Done changed from 0 to 40

- Estimated time set to 30.00

#6 - 2010-03-11 10:55 - Robert Lemke

- Status changed from New to Accepted

#7 - 2010-05-28 17:41 - Robert Lemke

- Target version deleted (1.0 alpha 9)

#8 - 2010-06-23 14:35 - Andreas Förthner

- Status changed from Accepted to Resolved

- % Done changed from 40 to 100

Applied in changeset r4613.