

TYPO3.Flow - Bug # 10718

Status:	Resolved	Priority:	Must have
Author:	Florian Kugler	Category:	Security
Created:	2010-11-10	Assigned To:	Karsten Dambekalns
Updated:	2010-11-15	Due date:	
PHP Version:			
Has patch:			
Complexity:			
Affected Flow version:			
Subject:	Content security: query rewriting fails if no other constraints are set on the query		
Description			
<p>The query rewriting aspect fails if the policy constraint is the only constraint on the query.</p> <p>In PersistenceQueryRewritingAspect::rewriteQomQuery() the policy constraint is added to the query by:</p> <pre>if (\$additionalCalculatedConstraints !== NULL) { \$newConstraints = \$query->logicalAnd(\$query->getConstraint(), \$query->logicalNot(\$additionalCalculatedConstraints)); \$query->matching(\$newConstraints); }</pre> <p>However, if \$query->getConstraint() returns NULL the call of logicalAnd() fails.</p> <p>This is my quick fix:</p> <pre>if (\$query->getConstraint() !== NULL) { \$newConstraints = \$query->logicalAnd(\$query->getConstraint(), \$query->logicalNot(\$additionalCalculatedConstraints)); } else { \$newConstraints = \$query->logicalNot(\$additionalCalculatedConstraints); }</pre>			

Associated revisions

Revision bc30a9d4 - 2010-11-12 16:28 - Karsten Dambekalns

[+BUGFIX] FLOW3 (Security): Fix query rewriting sans constraint

Adding the security constraint(s) failed if the original query did not have any constraint itself.

Change-Id: lcaa9534b1db4cb79dbf1114cdf7815b89e3bd5c1

Fixes: #10718

History

#1 - 2010-11-12 16:06 - Karsten Dambekalns

- Category set to Security
- Assigned To set to Andreas Förthner

Andi, any comments?

#2 - 2010-11-12 16:18 - Karsten Dambekalns

- *Status changed from New to Accepted*
- *Assigned To changed from Andreas Förthner to Karsten Dambekalns*

#3 - 2010-11-12 16:19 - Andreas Förthner

yep, this is correct. Fix looks good to me. @Karsten: Do we get this into alpha13, or is it already too late?

#4 - 2010-11-12 16:30 - Karsten Dambekalns

- *Status changed from Accepted to Under Review*

<http://review.typo3.org/330>

#5 - 2010-11-12 16:31 - Karsten Dambekalns

- *Target version set to 1.0 alpha 13*

#6 - 2010-11-13 22:08 - Karsten Dambekalns

Hi Florian,

it would be really cool if you could test the fix in <http://review.typo3.org/330>

Thanks, Karsten

#7 - 2010-11-15 11:15 - Karsten Dambekalns

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

Applied in changeset commit:"bc30a9d4360efa035e6656e05bd2e3c3c87efb47".