

TYPO3.Flow - Bug # 57410

Status:	Resolved	Priority:	Should have
Author:	Thomas Pilgaard Carlsen	Category:	MVC
Created:	2014-03-28	Assigned To:	Bastian Waidelich
Updated:	2014-04-02	Due date:	
PHP Version:			
Has patch:	No		
Complexity:			
Affected Flow version: Flow 2.0.0			
Subject:	initializeAction() can be called as controller action from request		
Description			
The following request can be called and without restriction:			
vendor.mypackage/standard/initialize			
Results in "Template Initialize.html could not be loaded"			
It seems to me that initializeAction should only be used internally in controller and should not be callable from request.			

Associated revisions

Revision 90132ee4 - 2014-03-31 15:38 - Bastian Waidelich

[BUGFIX] Prevent invocation of protected controller methods

Currently any method with an "Action" suffix is callable via the default request handling if a corresponding route exists.

For the fallback routes provided by Flow this is the case for the ``initialize*Action()`` methods that are called before the actual action invocation.

This change adds a check for the visibility of an action method and only allows invocation of public methods.

Change-Id: I076a56118b5fad112adf0dba0dee7b4711cfe903

Fixes: #57410

Releases: master, 2.2, 2.1

Revision 22212565 - 2014-04-02 15:32 - Bastian Waidelich

[BUGFIX] Prevent invocation of protected controller methods

Currently any method with an "Action" suffix is callable via the default request handling if a corresponding route exists.

For the fallback routes provided by Flow this is the case for the ``initialize*Action()`` methods that are called before the actual action invocation.

This change adds a check for the visibility of an action method and only allows invocation of public methods.

Change-Id: I076a56118b5fad112adf0dba0dee7b4711cfe903

Fixes: #57410

Releases: master, 2.2, 2.1

Revision b358926f - 2014-04-02 15:45 - Bastian Waidelich

[BUGFIX] Prevent invocation of protected controller methods

Currently any method with an "Action" suffix is callable via the default request handling if a corresponding route exists.

For the fallback routes provided by Flow this is the case for the ``initialize*Action()`` methods that are called before the actual action invocation.

This change adds a check for the visibility of an action method and only allows invocation of public methods.

Change-Id: I076a56118b5fad112adf0dba0dee7b4711cfe903

Fixes: #57410

Releases: master, 2.2, 2.1

History

#1 - 2014-03-28 14:01 - Thomas Pilgaard Carlsen

- *File bug-57410.patch added*

Made a patch.

#2 - 2014-03-28 15:12 - Alexander Berl

Wouldn't it maybe make sense to restrict it to public methods instead of hardcoding a special internal methodname (that might change in the future). Would need proper testing for performance, but it would be the more generic solution.

#3 - 2014-03-31 14:22 - Bastian Waidelich

- *Status changed from New to Needs Feedback*

Alexander Berl wrote:

Wouldn't it maybe make sense to restrict it to public methods instead of hardcoding a special internal methodname (that might change in the future). Would need proper testing for performance, but it would be the more generic solution.

I agree! Also the approach would not fix the problem for the action specific initialize-methods that you can implement (e.g. "initializeIndexAction()"). I just gave this a quick try and the following fix could work:

In the ActionController change 3 additional lines:

```
1 protected function resolveActionMethodName() {
2     // .....
3     if (!$this->reflectionService->isMethodPublic(get_class($this), $actionMethodName)) {
4         throw new NoSuchActionException(sprintf("The action \"%s\" in controller \"%s\" must be public!", $actionMethodName, get_class($this
5     ))), 1186669086);
6     }
7     // ...
8 }
```

Anyone feel free to push this to Gerrit (preferably with a test).

#4 - 2014-03-31 15:08 - Bastian Waidelich

- *Category set to MVC*
- *Status changed from Needs Feedback to Accepted*
- *Assigned To set to Bastian Waidelich*

#5 - 2014-03-31 15:38 - Gerrit Code Review

- *Status changed from Accepted to Under Review*

Patch set 1 for branch **master** of project **Packages/TYPO3.Flow** has been pushed to the review server.

It is available at <https://review.typo3.org/28979>

#6 - 2014-04-01 17:41 - Bastian Waidelich

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

Applied in changeset commit:90132ee42aa87c6d97c2bcbb5385bdc5b2fe9ddf.

#7 - 2014-04-02 15:32 - Gerrit Code Review

- *Status changed from Resolved to Under Review*

Patch set 1 for branch **2.2** of project **Packages/TYPO3.Flow** has been pushed to the review server.

It is available at <https://review.typo3.org/29076>

#8 - 2014-04-02 15:45 - Gerrit Code Review

Patch set 1 for branch **2.1** of project **Packages/TYPO3.Flow** has been pushed to the review server.

It is available at <https://review.typo3.org/29080>

#9 - 2014-04-02 16:42 - Bastian Waidelich

- Status changed from *Under Review* to *Resolved*

Applied in changeset commit:22212565c6a42a0387f354333b4742dac75138d1.

Files

bug-57410.patch

928 Bytes

2014-03-28

Thomas Pilgaard Carlsen