TYPO3.Flow - Bug # 27798

Status:	Accepted	**Priority:**	Must have
Author:	Karsten Dambekalns	**Category:**	Security
Created:	2011-07-01	**Assigned To:**	
Updated:	2013-08-14	**Due date:**	
PHP Version:			
Has patch:	No		
Complexity:	hard		
Affected Flow version:	FLOW3 1.0.0		
Subject:	CSRF protection not working for forms in a plugin		

Description

The CsrfProtectionAspect looks for package, subpackage, ... in the $arguments array, but for the request shown in the attached screenshot the information is one level below...

Related issues:

duplicated by TYPO3.Flow - Bug # 35720: Access denied Exception for widget li...	**New**	**2012-04-05**
duplicated by TYPO3.Fluid - Bug # 47078: widget.uri/linkViewHelpers fail with...	**Closed**	**2013-04-09**

Associated revisions

Revision 2a3bfd1e - 2012-07-13 12:01 - Bastian Waidelich

[TASK] Add HTTP status code to exceptions

Currently if an exception is rendered with either Debug-
or ProductionExceptionHandler the HTTP status is set to
"500 Internal Server Error".

This change adds a property "statusCode" to the FLOW3
base Exception allowing to set a custom HTTP status code.

This also sets status codes for some of the FLOW3 exceptions

Change-Id: Id65b7d78a2851953a448893f9dcfb2c63ddb2345
Related: #27798
Releases: 1.1, 1.2

Revision 3a8c98e9 - 2012-08-17 09:53 - Bastian Waidelich

[TASK] Add HTTP status code to exceptions

Currently if an exception is rendered with either Debug-
or ProductionExceptionHandler the HTTP status is set to
"500 Internal Server Error".

This change adds a property "statusCode" to the FLOW3
base Exception allowing to set a custom HTTP status code.

This also sets status codes for some of the FLOW3 exceptions

Change-Id: Id65b7d78a2851953a448893f9dcfb2c63ddb2345
Related: #27798
Releases: 1.1, 1.2

Revision 1b3a9e25 - 2012-09-05 16:09 - Bastian Waidelich

[BUGFIX] Throw exception on CSRF token error

Currently, if a required CSRF token is missing or invalid,
FLOW3 dies with a hard coded "Access denied!".

This change disables the try/catch blocks in the
RequestDispatchingAspect so that the access denied
exception is actually rendered.

This shouldn't pose a security issue as details are hidden
in production context.

Change-Id: I724b2332e2f8cecad8aa0414f98f3da824546f2e
Related: #27798
Releases: 1.1, 1.2

Revision 06777f7d - 2012-09-05 18:06 - Bastian Waidelich

[BUGFIX] Throw exception on CSRF token error

Currently, if a required CSRF token is missing or invalid,
FLOW3 dies with a hard coded "Access denied!".

This change disables the try/catch blocks in the
RequestDispatchingAspect so that the access denied
exception is actually rendered.

This shouldn't pose a security issue as details are hidden
in production context.

Change-Id: I724b2332e2f8cecad8aa0414f98f3da824546f2e
Related: #27798
Releases: 1.1, 1.2

History

#1 - 2011-10-20 01:43 - Karsten Dambekalns

- Target version deleted (1230)

#2 - 2011-10-21 13:20 - Karsten Dambekalns

- Affected Flow version set to FLOW3 1.0.0

#3 - 2012-01-06 17:57 - Bastian Waidelich

- Has patch set to No

They also do not work in widget (e.g. pagination does not work in protected actions!)

#4 - 2012-06-26 09:56 - Karsten Dambekalns

- Assigned To deleted (Andreas Förthner)

- Target version set to 1.1

#5 - 2012-06-26 14:21 - Bastian Waidelich

- Complexity set to hard

This is probably quite hard to solve because we needed to check all actions of a request and its sub requests. In Phoenix this could be as nested as:

```
FrontendNodeController::showAction() -> Plugin::fooAction() -> Widget::barAction()
```

As an intermediate work around one can add the @FLOW3\SkipCsrfProtection annotation to the affected actions as the CSRF token is there to prevent someone from sending a link that submits/changes data on the server with elevated permission level. So usually that is only relevant for "writing" actions (and those shouldn't contain pagination).

If this doesn't make it into 1.1 I'll take care of adding above hint to the exception message.

#6 - 2012-07-10 08:29 - Karsten Dambekalns

- Status changed from New to Needs Feedback

- Assigned To set to Bastian Waidelich

- Target version changed from 1.1 to 2.0 beta 1

Hi Bastian.

Bastian Waidelich wrote:

> *If this doesn't make it into 1.1 I'll take care of adding above hint to the exception message.*

Could you do this now?

#7 - 2012-07-11 11:27 - Bastian Waidelich

- Status changed from Needs Feedback to Accepted

Karsten Dambekalns wrote:

> *Could you do this now?*

I'll try. The challenge: We don't throw an exception yet. Instead this is the only(?) place where we die with "Access denied!" - But this should be improved anyways IMO.

#8 - 2012-07-12 17:16 - Bastian Waidelich

- Assigned To deleted (Bastian Waidelich)

Bastian Waidelich wrote:

> *Karsten Dambekalns wrote:*
>
> > *Could you do this now?*
>
> *I'll try.*

See https://review.typo3.org/#/c/12774 for a first work-around (not the final solution)

#9 - 2012-09-25 08:30 - David Sporer

Sorry stupid question...
I've deleted it.

#10 - 2012-12-12 09:20 - Karsten Dambekalns

- Target version changed from 2.0 beta 1 to 2.0

#11 - 2013-08-14 15:35 - Karsten Dambekalns

- Target version changed from 2.0 to 2.0.1

Files

plugin_-_csrf_-_arguments.png	468.3 kB	2011-07-01	Karsten Dambekalns