TYPO3.Flow - Bug # 29976

Status:	Resolved	**Priority:**	Must have
Author:	Bastian Waidelich	**Category:**	Security
Created:	2011-09-18	**Assigned To:**	
Updated:	2011-10-15	**Due date:**	
PHP Version:			
Has patch:			
Complexity:			
Affected Flow version:			
Subject:	CSRF token is always the same		

Description

This is probably a Windows issue (Windows 7, 64bit):
The blog example generates links like "posts/new?__csrfToken=00000000000000000000000000000000" for protected actions.

Associated revisions

Revision 1dd7ba68 - 2011-10-12 23:43 - Christian Müller

[BUGFIX] Security_Randomizer fallback does not work

This fix should allow Security_Randomizer to work on Win x64
by making sure that the mt_rand fallback actually returns random
bytes.

see http://sourceforge.net/tracker/?group_id=294448&atid=1243705
for more details

Change-Id: I93c432e45071a3c5628e98b3fbefa7407c715c15
Resolves: #29976

History

#1 - 2011-10-11 16:37 - Christian Müller

That is a shortcoming of /Packages/Framework/TYPO3.FLOW3/Resources/PHP/iSecurity/Security_Randomizer.php, it also mentions in a comment that it probably won't work on Win 64-bit.

#2 - 2011-10-11 16:38 - Christian Müller

Maybe we should add a fallback to generate "not so strongly randomized data" to have it running on Win 64-bit but log the fact that it is not so secure? WDYT?

#3 - 2011-10-11 17:01 - Bastian Waidelich

Christian Mueller wrote:

> *Maybe we should add a fallback to generate "not so strongly randomized data" to have it running on Win 64-bit but log the fact that it is not so secure? WDYT?*

+1
The Randomizer already comes with a fallback to mt_rand - but the problem is, that (in my case) it doesn't reach that fallback as it considers "00000000000000000000000000000000" as valid result.

#4 - 2011-10-11 19:31 - Christian Müller

Yep I see,

I guess it goes wrong around line 219 for you, maybe you check that out. It fills an array with zeros then uses the .NET crypto stuff, but finally it returns the array filled with zeros. For me this code looks plain wrong, I think this $variant thingy is filled with the random bytes and so its content needs to be returned there.

#5 - 2011-10-11 19:52 - Mr. Hudson

- Status changed from New to Under Review

Patch set 1 of change I93c432e45071a3c5628e98b3fbefa7407c715c15 has been pushed to the review server.
It is available at http://review.typo3.org/5727

#6 - 2011-10-12 12:46 - Bastian Waidelich

FYI: We have added two bug reports to the "Improved Security" project at SourceSorge

#7 - 2011-10-12 23:44 - Mr. Hudson

Patch set 2 of change I93c432e45071a3c5628e98b3fbefa7407c715c15 has been pushed to the review server.
It is available at http://review.typo3.org/5727

#8 - 2011-10-15 01:40 - Christian Müller

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

Applied in changeset commit:1dd7ba68d3f0b6d6b2c0f9ef9f480e80aab08f2d.