TYPO3.Flow - Bug # 6315

Status:	Resolved	**Priority:**	Should have
Author:	Robert Lemke	**Category:**	Security
Created:	2010-02-02	**Assigned To:**	Karsten Dambekalns
Updated:	2010-10-20	**Due date:**	
PHP Version:			
Has patch:			
Complexity:			
Affected Flow version:			
Subject:	Input fields with a name attribute with more than 64 characters are ignored		

Description

(by Fabian Guth)

Input fields with a name attribute with more than 64 characters are ignored.

After hours of digging into the Flow3-Code i realized that its possibly a wrong PHP setting. Following test case shows, that input fields with long (more than 64 characters) name attributes are ignored.

I would really appreciate any hints on the bad setting variable!
I searched php.ini and http.conf without success.

Test Case:

```
 <?php echo print_r($_POST); ?>

<form action= "" method="post">
 <input type="text"
name="aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"/>
 <input type="text"
name="bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb"/>
 <input type="submit" value="Submit"/>
</form>
```

Renders following after submit (both fields are filled):

```
Array
(
   [bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb] => b
)
```

As a workaround i edited the Token (F3\FLOW3\Security\Authentication\Token\UsernamePassword) to check for a short array key. I hope there aren't any side effects.
I know that it's better to subclass it with a changed "updateCredentials" method to preserve the patch at the next release.

As i use the default Linux PHP Package, i am afraid its a very common setting.

Associated revisions

Revision 31a541b1 - 2010-08-23 16:50 - Karsten Dambekalns

[+BUGFIX] FLOW3 (Security): Shortened some variable names in HTML (input fields with a name longer than 64 characters are ignored in default Suhosin setups), fixes #6315.

Change-Id: Id86ac9938d73dc40e58fae65b2c540e2f2252122

History

#1 - 2010-02-26 12:51 - Karsten Dambekalns

- Status changed from New to Needs Feedback

Do you have the Suhosin/Hardened PHP patch installed? Check phpinfo() to make sure, please.

#2 - 2010-02-26 13:03 - Fabian Guth

phpinfo() says:
This server is protected with the Suhosin Patch 0.9.8

#3 - 2010-03-02 11:40 - Robert Lemke

- Status changed from Needs Feedback to Closed

Can't reproduce this behavior on a machine without Suhosin enabled.

#4 - 2010-06-07 17:11 - Robert Lemke

- Status changed from Closed to Accepted
- Target version changed from 1.0 alpha 8 to 1.0 alpha 10

#5 - 2010-07-09 14:03 - Robert Lemke

- Status changed from Accepted to Needs Feedback
- Target version changed from 1.0 alpha 10 to 1.0 alpha 11

How can we solve / work around this?

#6 - 2010-08-18 16:14 - Karsten Dambekalns

- Status changed from Needs Feedback to Accepted
- Assigned To set to Karsten Dambekalns

To me it seems we should avoid such long names.

While it is not a security risk to have long names, Suhosin will continue to be popular und probably won't change it's defaults. That being said, the 64 char limit is for a variable name, in case of arrays that does not include the indices (the limit for the complete thing is 256). Thus it should be relatively easy to stay below that limit.

#7 - 2010-08-18 17:54 - Karsten Dambekalns

- Category changed from MVC to Security

One way for this (special) case of the authentication data: use a nested array instead of the long name. Equally unique and since we circumvent MVC argument handling in this case anyway, we can do this without side effects.

#8 - 2010-08-18 18:00 - Karsten Dambekalns

- Status changed from Accepted to Resolved

- % Done changed from 0 to 100

Applied in changeset r5005.