Core - Bug # 34964

Status:	Resolved	**Priority:**	Should have
Author:	Steffen Müller	**Category:**	
Created:	2012-03-17	**Assigned To:**	
Updated:	2013-05-28	**Due date:**	
TYPO3 Version:	4.5		
PHP Version:			
Complexity:			
Is Regression:			
Sprint Focus:			
Subject:	FE Session record is never removed, even if no session data left		

Description

One of the security features in TYPO3 is a changing FE cookie IDs for each request. This mechanism is paused when session data is saved. The problem is that there is no proper way to remove session data. Instead, entries are saved without valid data. So even if there is no more session data, the cookie stays unchanged, which undermines a security feature.

Flashmessages demonstrate the issue. Once a flashmessages was set in session data, it never gets removed. Even if it was delivered and flushed.

Invalidation of FE session data happens in tslib_feuserauth::storeSessionData()

```
...
$insertFields = array (
  'hash' => $this->id,
  'content' => serialize($this->sesData),
  'tstamp' => $GLOBALS['EXEC_TIME'],
);
$this->removeSessionData();
$GLOBALS['TYPO3_DB']->exec_INSERTquery('fe_session_data', $insertFields);
...
```

$this->sesData is NULL, but serialize($this->sesData) results in 'N;'.
However, even if it was NULL, the session data is never removed. There is no check for empty data.

Solution is to check for $data===NULL in setKey(), then unset the key and check for empty $this->sesData before writing to DB.

Related issues:

related to Core - Bug # 45578: storeSessionData not working anymore with 4.5.23	**Rejected**	**2013-02-18**
related to Core - Bug # 45570: fe_session Data Change external payment checkout	**Resolved**	**2013-02-18**
related to Core - Bug # 45708: feuserauth storeSessionData fails to save Data...	**Closed**	**2013-02-21**
related to Core - Bug # 53598: Select/Delete fe_sessions twice per request	**Resolved**	**2013-11-13**

Associated revisions

Revision b4a4cdd0 - 2012-12-04 14:42 - Steffen Müller

[BUGFIX] FE session records are never removed

The FE session records are never removed,
even if no session data are left.

Change-Id: Ibc281b2831567476dc0ba607de0753cd6ad39bc9
Fixes: #34964
Releases: 4.5, 4.6, 4.7, 6.0
Reviewed-on: http://review.typo3.org/9719
Reviewed-by: Markus Klein
Tested-by: Markus Klein
Reviewed-by: Stefan Neufeind
Reviewed-by: Dmitry Dulepov
Tested-by: Dmitry Dulepov

Revision 55bca032 - 2012-12-20 10:01 - Steffen Müller

[BUGFIX] FE session records are never removed

The FE session records are never removed,
even if no session data are left.

Change-Id: I5fcb9c7024ca0934e43f77a1310d559b715935c7
Fixes: #34964
Releases: 4.5, 4.6, 4.7, 6.0
Reviewed-on: https://review.typo3.org/16952
Reviewed-by: Dmitry Dulepov
Tested-by: Dmitry Dulepov

Revision 34af1041 - 2012-12-20 10:01 - Steffen Müller

[BUGFIX] FE session records are never removed

The FE session records are never removed,
even if no session data are left.

Change-Id: I152f565fcee27de09532a11d0342be4382509b28
Fixes: #34964
Releases: 4.5, 4.6, 4.7, 6.0, 6.1
Reviewed-on: https://review.typo3.org/16954
Reviewed-by: Dmitry Dulepov
Tested-by: Dmitry Dulepov

Revision d4d9e0d3 - 2012-12-20 10:03 - Steffen Müller

[BUGFIX] FE session records are never removed

The FE session records are never removed,
even if no session data are left.

Change-Id: Ib7a660beba5b4ce04543868ca31949cc15b064a4
Fixes: #34964
Releases: 4.5, 4.6, 4.7, 6.0, 6.1
Reviewed-on: https://review.typo3.org/16955
Reviewed-by: Dmitry Dulepov

Tested-by: Dmitry Dulepov

Revision da58b20c - 2012-12-20 10:03 - Steffen Müller

[BUGFIX] FE session records are never removed

The FE session records are never removed,
even if no session data are left.

Change-Id: Ic30acd00b9e5bfd09910d5e070b67f4dc865030e
Fixes: #34964
Releases: 4.5, 4.6, 4.7, 6.0, 6.1
Reviewed-on: https://review.typo3.org/16956
Reviewed-by: Dmitry Dulepov
Tested-by: Dmitry Dulepov

History

#1 - 2012-03-17 15:49 - Gerrit Code Review

- Status changed from New to Under Review

Patch set 1 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/9719

#2 - 2012-03-17 15:52 - Steffen Müller

- File 34964_4-5.diff added

Added also a patch for TYPO3 4.5

#3 - 2012-03-17 15:53 - Steffen Müller

The example code above is taken from 4.5, but the problem still exists in master.

#4 - 2012-03-17 16:12 - Steffen Müller

- File T3X_demo34964-0_0_0-z-201203171606.t3x added

Demo extension added.
Just install and add plugin to page.

1. Hit "Reload page" multiple times to see the cookie changing.
2. Hit "Add and show a Flashmessage" to add flash message.
3. Hit "Reload page" again multiple times to see the cookie is NOT changing anymore.

Apply patch and replay above steps.

#5 - 2012-03-17 16:19 - Steffen Müller

If you try to reproduce with server and client on localhost, you have to add this line to localconf.php:

```
$TYPO3_CONF_VARS['SYS']['devIPmask'] = '254.254.254.254';
```

#6 - 2012-03-18 17:30 - Philipp Gampe

With and without your patch, the displayed cookie is never changing unless I close the browser.

How do you make the cookie change?

#7 - 2012-03-18 18:41 - Helmut Hummel
- Status changed from Under Review to Needs Feedback

There's no benefit in changing the session id on every request. This is just a side effect of the session fixation prevention in combination with the currently implemented frontend session data logic.
It would be absolutely fine to have the same session id over several requests, especially when it's an unauthorized session, if it can be guaranteed that it is an id generated by TYPO3.

Just in contrast I would prefer to keep one id for unauthorized sessions and only regenerate it when a user logs in.

I think your patch would not harm, but I also do not see any benefits. Can you elaborate your point?

#8 - 2012-03-18 19:01 - Steffen Müller

Indeed, you are right. I will investigate and write a post as soon as I found the reason for this.

#9 - 2012-03-18 19:06 - Steffen Müller

Helmut, thanks for your feedback.
I was just wondering that flashmessages save bogus data to fe_session_data and that it changes behavior of cookie regeneration.

#10 - 2012-03-18 19:16 - Gerrit Code Review
- Status changed from Needs Feedback to Under Review

Patch set 2 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/9719

#11 - 2012-03-18 19:18 - Steffen Müller

I uploaded a new patch which also add a test for empty data in setKey()

I still have to investigate why the demo extension is not working.

#12 - 2012-03-18 19:40 - Gerrit Code Review

Patch set 3 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/9719

#13 - 2012-03-18 19:51 - Steffen Müller

Ok. Now the patch is finally complete and the demo extension should work, too.

#14 - 2012-03-19 12:54 - Gerrit Code Review

Patch set 4 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/9719

#15 - 2012-04-14 23:14 - Gerrit Code Review

Patch set 5 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/9719

#16 - 2012-10-31 00:01 - Gerrit Code Review

Patch set 6 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/9719

#17 - 2012-12-04 14:46 - Gerrit Code Review

Patch set 1 for branch **TYPO3_6-0** has been pushed to the review server.
It is available at http://review.typo3.org/16952

#18 - 2012-12-04 14:55 - Gerrit Code Review

Patch set 1 for branch **TYPO3_4-7** has been pushed to the review server.
It is available at http://review.typo3.org/16954

#19 - 2012-12-04 15:04 - Gerrit Code Review

Patch set 1 for branch **TYPO3_4-6** has been pushed to the review server.
It is available at http://review.typo3.org/16955

#20 - 2012-12-04 15:08 - Gerrit Code Review

Patch set 1 for branch **TYPO3_4-5** has been pushed to the review server.
It is available at http://review.typo3.org/16956

#21 - 2012-12-04 15:30 - Steffen Müller

- Status changed from Under Review to Resolved

- % Done changed from 0 to 100

Applied in changeset commit:b4a4cdd09679a0c34ec121fb18e8eafe0408449c.

#22 - 2013-02-18 17:08 - Johannes Goslar

The 4.5 patch seems to have an error: http://forge.typo3.org/issues/45578

#23 - 2013-05-28 02:37 - Elliot Sawyer

This issue was not included in 4.5.25 because it changes the behaviour. See by Oliver Hader's comment here: http://forge.typo3.org/issues/45570#note-7

Files

34964_4-5.diff	2.7 kB	2012-03-17	Steffen Müller
T3X_demo34964-0_0_0-z-201203171606.t3x	94.5 kB	2012-03-17	Steffen Müller