

## Core - Task # 55549

<b>Status:</b>	Resolved	<b>Priority:</b>	Should have
<b>Author:</b>	Benjamin Mack	<b>Category:</b>	Frontend
<b>Created:</b>	2014-02-01	<b>Assigned To:</b>	Benjamin Mack
<b>Updated:</b>	2014-02-06	<b>Due date:</b>	
<b>TYPO3 Version:</b>	6.2		
<b>PHP Version:</b>			
<b>Complexity:</b>			
<b>Sprint Focus:</b>			
<b>Subject:</b>	Only set FE user cookie if session data or user logged in		
<b>Description</b>	<p>Currently the FE session cookie is set on every request and since 4.2 the sessionID is generated again on every request unless the user is logged in. This is implemented for avoiding the security problem of the session fixation (see #19831).</p> <p>If an installation does not use FE session cookies at all, an option (TYPO3_CONF_VARS-&gt;FE-&gt;dontSetCookie) never sets the cookie.</p> <p>As the current behavior for non-logged-in FE calls is not usable, the behaviour is changed to only set the cookie if the user is logged in or the session data is modified. The last example is helpful for websites with e.g. a shopping cart on non-logged-in pages. Currently, if an extension is trying to implement the latter, the extension needs to hook or XCLASS the FrontendUserAuthentication class to set the cookie whenever needed.</p> <p>Additionally, the security problem still exists if the cookie is not set by TYPO3 itself, that's why the cookie can only be set if there is a valid entry in fe_user_sessions.</p> <p>if using external caching (e.g. reverse proxies), a "unneeded" cookie is always set currently, which extensions like EXT:moc_varnish or EXT:cachinfo mock to only set the cookie if needed.</p> <p>The attached patch removes the default-setting of a cookie in the frontend, and only triggers the setcookie() function when sessionData is added or a user is logged-in.</p>		
<b>Related issues:</b>			
related to Core - Bug # 55845: Wrong check removes FE cookie	<b>Resolved</b>	<b>2014-02-10</b>	
related to Core - Bug # 57751: Felogin session not set	<b>Resolved</b>	<b>2014-04-08</b>	

related to Core - Bug # 62100: I have no session cookie after using FE_SESSIO...	<b>Resolved</b>	<b>2014-10-08</b>
related to Core - Bug # 65223: FE Session for logged in user lost after empty...	<b>Resolved</b>	<b>2015-02-23</b>
related to Core - Bug # 63597: Felogin session cookie is destroyed when navig...	<b>New</b>	<b>2014-12-05</b>

## Associated revisions

### Revision 4d25aee5 - 2014-02-06 17:16 - Benjamin Mack

[TASK] Only set FE user cookie if session data or user logged in

Currently the FE session cookie is set on every request and since 4.2 the sessionID is generated again on every request unless the user is logged in. This is implemented for avoiding the security problem of the session fixation (see #19831).

If an installation does not use FE session cookies at all, an option (TYPO3\_CONF\_VARS->FE->dontSetCookie) never sets the cookie.

As the current behavior for non-logged-in FE calls is not usable, the behaviour is changed to only set the cookie if the user is logged in or the session data is modified. The last example is helpful for websites with e.g. a shopping cart on non-logged-in pages. Currently, if an extension is trying to implement the latter, the extension needs to hook or XCLASS the FrontendUserAuthentication class to set the cookie whenever needed.

Additionally, the security problem still exists if the cookie is not set by TYPO3 itself, that's why the cookie can only be set if there is a valid entry in fe\_user\_sessions.

if using external caching (e.g. reverse proxies), a "unneeded" cookie is always set currently, which extensions like EXT:moc\_varnish or EXT:cachinfo mock to only set the cookie if needed.

The attached patch removes the default-setting of a cookie in the frontend, and only triggers the setcookie() function when sessionData is added or a user is logged-in.

Resolves: #55549

Releases: 6.2

Change-Id: If478bc00c2c55dda0cc38a898a1288098891671f

Reviewed-on: <https://review.typo3.org/27230>

Reviewed-by: Markus Klein

Tested-by: Markus Klein

Reviewed-by: Wouter Wolters

Tested-by: Wouter Wolters

Reviewed-by: Benjamin Mack

Tested-by: Benjamin Mack

## Revision 00c895c0 - 2014-02-11 09:59 - Frans Saris

[BUGFIX] Wrong check removes FE cookie

Issue #55549 added a wrong check for user uid.  
As result the FE cookie gets deleted when you are  
loggedin instead when your not.

This change inverses the check.

Resolves: #55845

Releases: 6.2

Change-Id: I0c59afb8c89e9f7887970eaf0a4079fe98280b2c

Reviewed-on: <https://review.typo3.org/27525>

Reviewed-by: Wouter Wolters

Reviewed-by: Markus Klein

Reviewed-by: Marcin Sagol

Reviewed-by: Benjamin Mack

Tested-by: Benjamin Mack

## History

---

### #1 - 2014-02-01 13:48 - Gerrit Code Review

- Status changed from New to Under Review

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

It is available at <https://review.typo3.org/27230>

### #2 - 2014-02-01 14:26 - Gerrit Code Review

Patch set 2 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.

It is available at <https://review.typo3.org/27230>

### #3 - 2014-02-01 14:39 - Gerrit Code Review

Patch set 3 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.

It is available at <https://review.typo3.org/27230>

### #4 - 2014-02-01 14:41 - Gerrit Code Review

Patch set 4 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.

It is available at <https://review.typo3.org/27230>

### #5 - 2014-02-04 23:49 - Gerrit Code Review

Patch set 5 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.  
It is available at <https://review.typo3.org/27230>

**#6 - 2014-02-05 13:38 - Gerrit Code Review**

Patch set 6 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.  
It is available at <https://review.typo3.org/27230>

**#7 - 2014-02-05 17:43 - Gerrit Code Review**

Patch set 7 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.  
It is available at <https://review.typo3.org/27230>

**#8 - 2014-02-06 17:30 - Benjamin Mack**

- *Status changed from Under Review to Resolved*

- *% Done changed from 0 to 100*

Applied in changeset commit:4d25aee5587b167e1676c8e59147b13b18a9a02d.