Core - Bug # 19867

Status:	Resolved	**Priority:**	Must have
Author:	Marcus Krause	**Category:**	
Created:	2009-01-20	**Assigned To:**	Michael Stucki
Updated:	2009-01-24	**Due date:**	
TYPO3 Version:	4.0		
PHP Version:	5.2		
Complexity:			
Is Regression:			
Sprint Focus:			
Subject:	DB session records are only created when users authenticate		

Description

Functions $GLOBALS["TSFE"]->fe_user->getKey() or $GLOBALS["TSFE"]->fe_user->setKey() allow to bind data to a user's session. Unfortunately TYPO3 only creates DB session records in tables be_sessions/fe_sessions if a user authenticates.

Before applying the session fixation fix, TYPO3 always trusted the session id provided by the user through COOKIE etc. Although no DB session records were created, setKey() and getKey() worked in a way that a record in fe_session_data was created (including session id) and could be accessed.

Now, after the session fixation fix, TYPO3 will issue a new session id if there's no according db record in be_sessions/fe_sessions. This now has the drawback that every request of a non-authenticated user will force TYPO3 to issue a new session id so that getKey() no longer works as existing records in fe_session_data are associated to an "old" session identifier.

I believe that the security fix is not the cause of the problem but the trigger for it. I expect TYPO3 to create a DB session record whenever a session id is generated not only when a user authenticates itself.

(issue imported from #M10205)

Related issues:

related to Core - Bug # 19831: Session fixation vulnerability in user authent...	**Resolved**	**2009-01-15**
duplicated by Core - Bug # 19880: Patch 10146 in Version 4.2.4 does not work ...	**Resolved**	**2009-01-21**
duplicated by Core - Bug # 19874: Typo3 4.1.8: fe_session_data regression due...	**Resolved**	**2009-01-21**
duplicated by Core - Bug # 19879: after upgrade from 4.1.7 to 4.1.8 feusers a...	**Resolved**	**2009-01-21**

History

#1 - 2009-01-20 23:20 - Marcus Krause

There are two possible solutions:

- let method isExistingSessionRecord() check both tables fe_sessions/be_sessions AND fe_session_data for existing session ids
or
- let TYPO3 create be_sessions/fe_sessions records also for non-authenticated users

My favourite is #2; what do you think?

#2 - 2009-01-21 09:58 - Francois Suter

Solution 2 seems more consistent.Obviously session ids need to be preserved once the user is logged in.

#3 - 2009-01-21 12:56 - Dmitry Dulepov

#2

#4 - 2009-01-21 12:59 - Dmitry Dulepov

Uploaded a simple script to test&reproduce the problem. The following TS should be added to the site TS to see it in action:

```
includeLibs.user_sestest = fileadmin/user_sestest.php
page.5 = USER_INT
page.5.userFunc = user_sestest
```

The output will display previous and new value (time stamp actually). With older TYPO3 code both values were shown. Current trunk shows only the new value (old one is always empty).

#5 - 2009-01-21 15:12 - Christian Hernmarck

Just a note:
this bug/topic is important - I upgraded to Typo3 4.0.10, 4.1.8 and 4.2.4 (several installations on several servers) and later realized that the shop is not working anymore (basket always empty).
Maybe my fault (I didn't check everything on the new version) - but it seems that the updates are more and more problematic...

Regards
Christian

#6 - 2009-01-21 17:45 - Daniel Hahler

WORKAROUND:

comment out / remove this part in t3lib/class.t3lib_userauth.php:
"|| !$this->isExistingSessionRecord($id)"

This removes the "session fixation fix" and appears to be better than downgrading completely.

#7 - 2009-01-21 19:23 - Steffen Kamper

i see this patch as very urgent. The releases are not working and new release has to come very soon.
Does this patch brings the usersession back?

#8 - 2009-01-21 20:27 - Marcus Krause

There is no patch so far, just a workarround that reverts the session fixation fix.

#9 - 2009-01-21 20:47 - Steffen Kamper

i tend to #2, but i think there must be a garbage collection as this can raise data a lot, especially the anonymous session data should be deleted after

some hours/days.

Unfortunally we need a quick fix.

#10 - 2009-01-21 21:30 - Helmut Hummel

I'm not too happy about storing *every* anonymous session into the database. This could lead to a serious performance impact an high traffic sites.
So, I would vote for solution #1 to avoid unnecessary load on the server.

A compromise would be to only store the session id in fe_sessions, if $this->sesData_change is set and data is written to fe_sessions_data table...

But I'm not sure on this ...

#11 - 2009-01-21 21:55 - Steffen Kamper

for the urgent reason i would say:

- use #1 for now to have a fix.
- work on an alternative way like #2 without hurry

#12 - 2009-01-21 21:56 - Marcus Krause

So it's currently unclear; both solution have their pros and cons.

I hereby unassign this issue. I don't want to stop anybody to work on it.

#13 - 2009-01-21 22:48 - Marcus Krause

Hotfixes added, please test!

(*_trunk.diff is for subversion trunk only)

#14 - 2009-01-22 01:09 - Ralph Brugger

Hotfix 10205.diff tested for www.bobsairport.de
Seems to work!
Thanks for the fast hotfix

#15 - 2009-01-22 02:24 - Daniel Hahler

re patch: I think the additional check should only get done, if "! $count" applies to the first check;
In case there are results already from the first check, the second one can be skipped (saves a query).
Otherwise this patch looks good.

#16 - 2009-01-22 10:02 - Franz Holzinger

tt_products basket: The patch 10205_trunk.diff for the trunk works fine, but only tt_products 2.8.0. It does not work with tt_products 2.5.10.

The patch 10205.diff for TYPO3 4.2.4 does not change anything. The table fe_session_data always remains empty.

#17 - 2009-01-22 11:38 - Manfred Mueller-Spaeth

The problem comes in another "flavour" for me: fe_users may login, but on the next request, they seem to be logged out.

The workaround mentioned above works fine in this case, but not the hotfix 10205.diff, this won't change anything on the problem described above.

Edit: TYPO3 4.2.4 - PHP 5.2.x - tested with FireFox on Mac OS X and Windows

Edit: Sorry, I made a mistake, now the hotfix works fine!

#18 - 2009-01-22 12:45 - Michael Fritz

Thanx alot!! the hotfix does the trick!

10205.diff [^] (858 bytes) 21.01.09 23:47

#19 - 2009-01-22 17:36 - Michael Stucki

By having a look at patch "10205.diff" I think it is not solving the problem correctly.

1) Although such session information is most likely stored in FE sessions only, there is no guarantee for this. At least checking the ->loginType is the wrong way in my opinion.

2) Instead of doing a select query in the fe_session_data table, I propose to simply check the client session lifetime. Every value which is more than 0 should have a corresponding record in fe_session, and vice versa, if the lifetime is 0 we can be sure it's a non-authenticated session.

Those who tried the old patch already, please re-test if the new solution from "bug_10205_v2.diff" will also work for you. Thanks in advance!

- michael

#20 - 2009-01-22 18:01 - Ralph Brugger

I've checked bug_10205_v2.diff too for bobsairport.de.
It seems be working the same way as the old bug_10205.diff patch.
Sessions are created the right way, and none existing sessions are also detected.
=> it works 4 me:)

#21 - 2009-01-22 18:34 - Franz Holzinger

Patch bug_10205_v2.diff is not against current svn trunk, as I have thought.
Could you please attach the patch for trunk?

#22 - 2009-01-22 18:35 - Steffen Kamper

I tested v2 with trunk. I had the problem that i can't login in BE (i logged in and session was invalid direct after login). Applying the patch BE login works

again.

#23 - 2009-01-22 18:37 - Steffen Kamper

I attached the v2-patch for trunk

#24 - 2009-01-22 18:43 - Marcus Krause

v2 is broken, it again allows session fixation for non-authenticated (fe-) users

#25 - 2009-01-22 20:57 - Reto Schmid

I test the new Patch "bug_10205_v2.diff", and it's look's good!

tt_products runs and no problems with logins ...

Thanks a lot ;)

#26 - 2009-01-22 23:20 - Ben van 't Ende

After the fix we had no problems either. Will this be a HOTFIX now?

#27 - 2009-01-22 23:22 - Steffen Kamper

we have to check comment from Marcus first as this would be a no-go

#28 - 2009-01-22 23:36 - Marcus Krause

I've reviewed a new patch created by Michael. This patch seems to be a proper bugfix. I guess, he will add it here very soon.

#29 - 2009-01-23 09:04 - Michael Stucki

New patch mentioned by Marcus is up now (bug_10205_v3.diff). Please test once again...

#30 - 2009-01-23 10:47 - Clemens Kalb

bug_10205_v3.diff didn't fix the problem described by Manfred Mueller-Spaeth a few comments earlier (at least it didn't fix it for me): fe_users may login, but on the next request, they seem to be logged out (TYPO3 4.0.10).

#31 - 2009-01-23 11:46 - Jens Hirschfeld

[Update]
I've tested the patch bug_10205_v3.diff.
To reproduce the Problem with the login being not possible with the patch bug_10205_v3.diff:

1. go to the fe-login page.
2. delete your fe_typo_user cookie
3. login (it looks like it is successful)
4. click any link in your page. You aren´t logged in any more.

How the login is possible:
1. delete your fe_typo_user cookie
2. go to any page on your site, which contains an extension, which saves session-data.
3. now go to the fe-login page.
4. login -> the login IS successful
[/Update]

[Wrong, don´t read it!]
This Part of the Note is wrong:
I've tested the patch bug_10205_v3.diff on different server (2x IIS and 1x Apache).

The patch worked on the Apache Server, but on IIS Server I have encountered the Problem, that no FE-User can log in!
The user types in the username in password. After clicking the "login" Button/Link the User is again on the "login" page.

If i replace the patched Files with the original ones, the login is again possible.
[/Wrong, don´t read it!]
The reason was, that on the IIS-Systems i had´nt already a cookie with Session-Data. On the Apache-System i did.

#32 - 2009-01-23 12:30 - Manfred Mueller-Spaeth

I thought all went fine, but I'm wrong ...

It's a curious thing: after using the system with the workaround above (just commenting out the call of "isExistingSessionRecord") and then patching the file (made unchanged again before), all works fine, also with deleted cookies. That's what I wrote yesterday in my comment.

But after truncating fe_session and fe_session_data, the same behaviour came up: fe_user login possible, but "forgotten login" with the next request.

Because of the lack of time, for the moment my description is not very precise. If no solution is found, I will track it with more details begin of next week.

#33 - 2009-01-23 12:37 - Benno Weinzierl

bug_10205_v3.diff did fix my 4.1.8-Installation.

It is a realy urgent matter as i also updated over 10 Projects until i noticed the disaster. There should be a Warning at the download-Page of www.typo3.org until this is fixed... just to prevent others to do the same mistake that i did.

Edit: Sorry, patch does NOT work in IE6&7. Users are only logged in for one request. => i think same thing as Manfred Mueller-Spaeth

#34 - 2009-01-23 22:26 - Michael Stucki

Finally found the reason why this works on some sites and and some it doesn't. My assumption regarding $lifetime was wrong. It is no indication for a non-authenticated user.

Therefore I'm uploading a new patch which doesn't have this condition and should finally work for all scenarios.

#35 - 2009-01-23 22:29 - Michael Stucki

bug_10205_v4.diff is tested and will be submitted to the core list next.

#36 - 2009-01-24 01:08 - Manfred Mueller-Spaeth

I'm really sorry ... but it's the same erroneous behaviour as before ...

After patching a freshly unzipped 4.2.4 with v4 and clearing all caches in TYPO3 as well as the cookies and sessions in the browser (FireFox) and emptying fe_sessions and fe_session_data, it's the same problem: a fe_user may login, but the next request on a secured page causes an error "The page did not exist or was inaccessible. Reason: ID was not an accessible page" as always.

Again: if there are sessions in the table from using the workaround above (commenting out the part " || !$this->isExistingSessionRecord($id)", the login works correctly without the workaround though. It's curious.

#37 - 2009-01-24 01:55 - Michael Stucki

Oh well... What a mess!

After verifying the patch on a clients site, I can confirm that it
works, however there are still more problems to be resolved.

The extension "commerce" does for some reason use its own session
table, meaning there is no content in fe_session, no content in
fe_session_data, but there is content in tx_commerce_baskets!

Now the question is, how should we treat that situation:

a) Ignore but warn users of that extension
b) Add a fix for commerce to the core - see attached patch
c) Add a configuration flag that disables the session fixation fix (so
   that the user gets more time to wait for a fix from the commerce
   developers).

Attached is a post patch that implements a check for the commerce
extension. However, what if there are more such extensions playing their
own game?

What do you propose?

- michael

#38 - 2009-01-24 10:10 - Michiel Roos

C
Extensions should definitely not bloat the core.

Sending a warning to the commerce team is fine too.

#39 - 2009-01-24 13:39 - Franz Holzinger

A hook can be added to allow this for multiple extensions.

#40 - 2009-01-24 16:58 - Ingmar Schlecht

Patch v5 committed to all affected branches.

Files

user_sestest.php	236 Bytes	2009-01-21	Administrator Admin
10205_trunk.diff	705 Bytes	2009-01-21	Administrator Admin
10205.diff	858 Bytes	2009-01-21	Administrator Admin
bug_10205_v2_trunk.diff	1.1 kB	2009-01-22	Administrator Admin
bug_10205_v3.diff	2.4 kB	2009-01-23	Administrator Admin
bug_10205_v4.diff	1.8 kB	2009-01-23	Administrator Admin
bug_10205_post1_commerce.diff	790 Bytes	2009-01-24	Administrator Admin
bug_10205_v5.patch	2.6 kB	2009-01-24	Administrator Admin