

TYPO3 Core - Bug #17120

Content is not cached and white page displayed with big content / PHP 5.2.1

2007-03-14 13:28 - Robert Lemke

Status:	Closed	Start date:	2007-03-14
Priority:	Should have	Due date:	
Assignee:	Dmitry Dulepov	% Done:	0%
Category:	Content Rendering	Estimated time:	0.00 hour
Target version:		Complexity:	
TYPO3 Version:		Is Regression:	
PHP Version:		Sprint Focus:	
Tags:			

Description

This problem originally occurred on typo3.org (ter_doc_pi1) but can be reproduced independently:

If a frontend plugin returns a large amount of content, this content is not written into the page cache. In addition not even the page without the FE plugin output is shown, but instead only a white page is displayed (which will be cached).

Use the attached extension to reproduce the behaviour:

- Install the FE plugin from the exploit extension on any page
- Make sure that you're running PHP 5.2.1
- View the page containing the FE plugin, the page should be blank
- Set the no_cache flag in the page properties or add "no_cache=1" to the GET parameters
- View the page containing the FE plugin, the page should display the content

Obviously the problem has nothing to do with the FE plugin itself (hence the exploit extension). While debugging, it turned out that in tslib_fe->setPageCacheContent() the \$content is already empty: Therefore the empty content is (correctly) stored in the cache_pages table.

The content disappears somewhere between the "return" of the FE plugin in the setPageCacheContent method in tslib_fe. (issue imported from #M5221)

History

#1 - 2007-03-14 13:30 - Robert Lemke

Additional note: For some reason the caching seems only to fail with the HTML content I put into the exploit extension (which is the real content which should be rendered at typo3.org). If I replace the HTML content by some generated string (with str_repeat) of a similar size, the whole caching DOES work.

#2 - 2007-03-14 17:58 - Popy no-lastname-given

No bug on my server.

I think the bug occurs in tsfe->generatePage_postProcessing, due to tidy or XHTMLcleaning :)

#3 - 2007-03-14 18:19 - Sebastian Kurfuerst

Do you have PHP 5.2.1 [Popy no-lastname-given](#)?

#4 - 2007-03-14 18:41 - Robert Lemke

[Popy no-lastname-given](#): Not a bad guess! I found it ...

It's not Tidy or the XHTML cleaning but it is some postprocessing. The function prefixLocalAnchorsWithScript() in tslib_fe consists of these two lines:

```
$scriptPath = substr(t3lib_div::getIndpEnv('TYPO3_REQUEST_URL'), strlen(t3lib_div::getIndpEnv('TYPO3_SITE_URL')));  
$this->content = preg_replace('/(<(a|area).*?href=")(#[^"]*)/i','$1' . htmlspecialchars($scriptPath) . '$3',$this->content);
```

The problem is that - at least with the HTML rendered by ter_doc_pi1 - the regular expression returns an empty string.

For now I disabled this function with "config.prefixLocalAnchors >". Now it's up to someone else checking the regular expression and it's dependency on a certain PHP version ...

#5 - 2007-03-14 18:42 - Robert Lemke

I can confirm this bug myself ;-) at least on three different servers ...

#6 - 2007-03-15 11:35 - Dmitry Dulepov

Possible solution described here:

<http://lists.netfielders.de/pipermail/typo3-team-typo3org/2007-March/002238.html>

#7 - 2008-10-29 16:19 - Daniel Hahler

Seems like "\$" should get escaped in the \$scriptPath/Request URI (regarding the linked post above).

But in general, I think this should get duped to bug 0006415.

#8 - 2008-12-18 20:03 - Dmitry Dulepov

Currently the code just sets original content back if new content is empty

#9 - 2018-10-02 12:32 - Benni Mack

- Status changed from Resolved to Closed

Files

T3X_user_cachebugexploit-0_0_0-z-200703141318.t3x	39.2 KB	2007-03-14	Administrator Admin
---	---------	------------	---------------------