TYPO3 Core - Bug #23521

Flash Uploader does not work if cookieHttpOnly is enabled

2010-09-09 13:10 - Oliver Hader

Status:	Rejected	**Start date:**	2010-09-09
Priority:	Should have	**Due date:**	
Assignee:	Steffen Gebert	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
TYPO3 Version:	4.5	**Complexity:**	
PHP Version:	5.2	**Is Regression:**	
Tags:		**Sprint Focus:**	

Description

The Flash Uploader does not work if the TYPO3_CONF_VARS setting "cookieHttpOnly" is enabled. After uploading a file, the uploader just shows a "303" error.

"303" is a HTTP status code and tells that there was a redirect since the backend user could not be authorized to have access to the TYPO3 backend.

(issue imported from #M15673)

Related issues:

Related to TYPO3 Core - Bug #22185: Flash Uploader not working in FF, SF and ...	**Closed**	**2010-02-25**
Related to TYPO3 Core - Feature #24647: Enable cookieHttpOnly by default	**Closed**	**2011-01-18**
Has duplicate TYPO3 Core - Bug #23419: Flash uploader doesn't work with cooki...	**Closed**	**2010-08-22**
Has duplicate TYPO3 Core - Bug #24654: Do not enable FlashUploader wenn cooki...	**Closed**	**2011-01-19**

History

#1 - 2010-09-09 13:17 - Oliver Hader

Find a first version for TYPO3 4.5 attached...
Still some work needs to be done to define the general concept of the new veriHash (also the name is not optimal yet)...

#2 - 2010-09-09 14:40 - Oliver Hader

Attached new patches that work without changes to the database.
However, I'm not sure whether DBAL can handle "MD5" correctly back in TYPO3_4-3...

#3 - 2010-09-10 12:48 - Oliver Hader

MD5 cannot be handled by DBAL, so we have to store the hash used for looking up records in the database as well (which means, that we cannot have a fix for already released TYPO3 versions). Furthermore it must be ensured that no new cookie will be set (since it transfers the session id in a not wanted scenario).

#4 - 2010-09-28 15:19 - Peter Russ

Patch v2_43 not working neither in IE nor FF. In both browser not upload, HTTP error 303 and logout from BE.

#5 - 2010-11-19 09:42 - Janos

Tested patch 0015673_v2_44.patch
Worked on:
FF 3.6.12
Chrome 7.0.....

For IE 8 i have the old, non js / flash, Upload system!? But I am not shure if this depends on the non, or miss-configured ie.

#6 - 2011-01-19 01:31 - Helmut Hummel

With this patch it is possible to get a valid session by knowing the idHash value. Thus the idHash is the new session id transmitted by GET.

Would be better to create one time tokens instead (like in the new CSRF protection in 4.5)

#7 - 2012-01-15 12:38 - Helmut Hummel

- File 23521_v3_45.diff added

- Target version deleted (0)

Even better just send the session id as a post value

#8 - 2012-01-16 16:14 - Helmut Hummel

Hm, actually my suggestion is equal to Olly's but just straight forward uses the session id, not a hash of it. But I think that's still OK.

#9 - 2012-03-10 12:17 - Steffen Müller

@Helmut: Any news from Amir about your solution? He promised to give feedback.

#10 - 2012-05-10 10:22 - Gerrit Code Review

- Status changed from Accepted to Under Review

Patch set 1 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/11124

#11 - 2012-05-10 15:44 - Gerrit Code Review

Patch set 2 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/11124

#12 - 2012-05-16 20:31 - Helmut Hummel

Steffen Müller wrote:

> @Helmut: Any news from Amir about your solution? He promised to give feedback.

Unfortunately not. However I figured out, why this might not be a good idea to do so :(

The idea of setting http_only to the cookie is to disallow JavaScript access to the cookie, which basically holds the session id.

If we now output it in the HTML, then the id is accessible again through JavaScript which will cancel the http_only protection of the cookie.

I have now no idea any more how to solve this.

#13 - 2012-08-29 15:04 - Florian Seirer

Just an idea (and it may sound silly), and I know this would be more work than just "fixing a bug":

Does the uploader have to rely on Flash? Or is there another, better, HTML5-kind-of way of uploading files to TYPO3?

#14 - 2012-08-29 15:57 - Steffen Gebert

Not silly at all. We have a HTML5 version already in TCEforms. There were also prototypes of plupload available.

#15 - 2013-02-26 12:22 - Lorenz Ulrich

Since the patch was abandoned, I suggest to close this issue as not fixable.

#16 - 2013-02-26 20:54 - Steffen Gebert

- Status changed from Under Review to Rejected

- Assignee changed from Oliver Hader to Steffen Gebert

Files

0015673.patch	5.6 KB	2010-09-09	Administrator Admin
0015673_v2_44.patch	4.07 KB	2010-09-09	Administrator Admin
0015673_v2_trunk.patch	4.05 KB	2010-09-09	Administrator Admin
0015673_v2_43.patch	4.4 KB	2010-09-09	Administrator Admin
23521_v3_45.diff	1.45 KB	2012-01-15	Helmut Hummel