Security Guide - Task # 59030

Task # 60744 (Closed): Raise version of TYPO3 Security Guide to 1.0.6

Status:	Closed	**Priority:**	Should have
Author:	Michael Schams	**Category:**	Guidelines for Integrators
Created:	2014-05-22	**Assigned To:**	Michael Schams
Updated:	2014-08-04	**Due date:**	
Subject:	Explain 'trustedHostsPattern' configuration option		

Description

In TYPO3 CMS 6.2.3, a new configuration option has been introduced:

    $GLOBALS['TYPO3_CONF_VARS']['SYS']['trustedHostsPattern']

This option can contain either the value "SERVER_NAME" or a regular expression pattern that matches all host names that are considered trustworthy for the particular TYPO3 installation. "SERVER_NAME" is the default value shipped with the above mentioned TYPO3 versions. With this option value in effect, TYPO3 checks the currently submitted host-header against the SERVER_NAME variable.

Further details:
http://typo3.org/teams/security/security-bulletins/typo3-core/typo3-core-sa-2014-001/

And discussions in the following thread (**Core mailing list**):
http://lists.typo3.org/pipermail/typo3-team-core/2014-May/055815.html

The task is to determine, if it is worth to explain the 'trustedHostsPattern' setting in the Security Guide (e.g. outline, what you should or should not configure to achieve a secure TYPO3 setup) - and possibly extend the Security Guide accordingly.

History

#1 - 2014-05-22 15:13 - Jo Hasenau

After upgrading the TYPO3 sources we ran into "Exception thrown without a stack frame blah" without any additional info.

Frontend and backend are running on NGINX behind an NGINX based HA-Proxy and the domains are configured to be running on different ports than default.
So the default setting SERVER_NAME just broke any TYPO3 instance completely and we just found out by accident, what the problem is.

The "accident" was a redirect which is activated for URLs without a trailing slash and it redirects from

    blah.domain.com/typo3

to

    blah.domain.tld:12345/typo3/

The latter was running smoothly, which lead us to the actual problem.

Setting the pattern to

    .*\.domain\.tld:*

finally solved the problem.

#2 - 2014-05-22 20:46 - Chris topher

Thanks for creating this issue so quickly, Michael!

> *The task is to determine, if it is worth to explain the 'trustedHostsPattern' setting in the Security Guide*

I don't have details on what to document currently, but I agree: *I* also thought it would make sense to add a few notes about this setting to the docs.

#3 - 2014-05-23 11:12 - Thomas Kieslich

for multi Domain Setup you can use regex style

'trustedHostsPattern' => '.*\.example|testing\.org|com:*',

#4 - 2014-06-23 14:07 - Michael Schams
- Status changed from New to Accepted
- Assigned To set to Michael Schams
- Target version set to 1.0.6
- Estimated time set to 1.00
- Remaining (hours) set to 1.0

#5 - 2014-06-23 14:13 - Michael Schams
- Category set to Guidelines for Integrators

#6 - 2014-08-01 12:18 - Francois Suter
- Remaining (hours) deleted (1.0)

Hey Michael, just checking. Any plan for publishing this one (and version 1.0.6 in general)?

BTW don't forget that the manuals are now on Github ;-)

#7 - 2014-08-02 14:31 - Michael Schams
- Status changed from Accepted to Under Review
- % Done changed from 0 to 80

My suggestion:

```
TYPO3 uses the HTTP header "Host:" to generate absolute URLs in several
places such as 404 handling, http(s) enforcement, password reset links
and many more. Since the host header itself is provided by the client,
it can be forged to any value, even in a name based virtual hosts
environment.
```

The "trustedHostsPattern" configuration option can contain either the
value *SERVER_NAME* or a regular expression pattern that matches all
host names that are considered trustworthy for the particular TYPO3
installation. "SERVER_NAME" is the default value and with this option
value in effect, TYPO3 checks the currently submitted host-header
against the SERVER_NAME variable. Please see security bulletin
TYPO3-CORE-SA-2014-001 for further details about specific setups.

The PHP variable reads: $TYPO3_CONF_VARS['SYS']['trustedHostsPattern']

Requires review from Security Team (Helmut?).

#8 - 2014-08-02 14:32 - Michael Schams

- File task59030-1.patch added

- File task59030-1.patch added

#9 - 2014-08-02 14:43 - Michael Schams

- Parent task set to #60744

#10 - 2014-08-04 11:53 - Michael Schams

- File task59030-2.patch added

- Status changed from Under Review to Needs Feedback

- Assigned To changed from Michael Schams to Helmut Hummel

- File task59030-2.patch added

Updated wording based on a suggestion by Helmut:

TYPO3 uses the HTTP header "Host:" to generate absolute URLs in several
places such as 404 handling, http(s) enforcement, password reset links
and many more. Since the host header itself is provided by the client,
it can be forged to any value, even in a name based virtual hosts
environment.

The "trustedHostsPattern" configuration option can contain either the
value *SERVER_NAME* or a regular expression pattern that matches all
host names that are considered trustworthy for the particular TYPO3
installation. "SERVER_NAME" is the default value and with this option
value in effect, TYPO3 checks the currently submitted host-header
against the SERVER_NAME variable. Please see security bulletin
`TYPO3-CORE-SA-2014-001 <http://typo3.org/teams/security/security-bulletins/typo3-core/typo3-core-sa-2014-001/>`_
for further details about specific setups.

If the "Host:" header also contains a non-standard port, the
configuration must include this value, too. This is especially important
for the default value "SERVER_NAME" as provided ports are checked
against SERVER_PORT which fails in some more complex load balancing
or SSL termination scenarios.

The PHP variable reads: $TYPO3_CONF_VARS['SYS']['trustedHostsPattern']

Requires review from Security Team (Helmut?).

#11 - 2014-08-04 13:03 - Helmut Hummel

looks good now, thanks!

#12 - 2014-08-04 13:59 - Michael Schams

- Status changed from Needs Feedback to Closed

- Assigned To changed from Helmut Hummel to Michael Schams

- % Done changed from 80 to 100

TYPO3 Security Guide v1.0.6 published - closing ticket as resolved.

Files

task59030-1.patch	1.5 kB	2014-08-02	Michael Schams
task59030-2.patch	1.8 kB	2014-08-04	Michael Schams