Security Guide - Task # 57144

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

Status:	Closed	**Priority:**	Should have
Author:	Helmut Hummel	**Category:**	Guidelines for Administrators
Created:	2014-03-21	**Assigned To:**	Michael Schams
Updated:	2014-08-04	**Due date:**	
Subject:	Configuration to add HTTP Headers to backend responses		

Description

It has been made possible to configure additional HTTP headers
to be sent in every backend request.

This mainly has been done to add a X-Frame-Options: SAMEORIGIN header for click jacking protection,
but it can also be used to let TYPO3 send additional headers in every backend request:

This code can be placed in ext_localconf.php or AdditionalConfiguration.php
$TYPO3_CONF_VARS['BE']['HTTP']['Response']['Headers'][] = 'X-Custom-Header: Value';

Related issues:

related to Core - Bug # 54201: Implement Clickjacking Protection	**Resolved**	**2013-12-04**

History

#1 - 2014-03-21 12:49 - Helmut Hummel

Disabling the clickjacking protection is not recommended but might be needed e.g. if you need to embed backend pages in iframes on a foreign domain.

Then the header can be reset by adding the following code:
unset($TYPO3_CONF_VARS['BE']['HTTP']['Response']['Headers']['clickJackingProtection']);

#2 - 2014-03-21 19:15 - Ernesto Baschny

Note that this setting was introduced in TYPO3 CMS 6.2, in case you are wondering. :)

#3 - 2014-03-22 13:04 - Francois Suter

- Project changed from Documentation to Security Guide

We don't have any manual describing all the TYPO3_CONF_VARS options, but I think this one fits very nicely into the Security Guide.

#4 - 2014-03-22 13:05 - Francois Suter

- Target version set to 1.0.5

#5 - 2014-03-22 13:31 - Michael Schams

- Status changed from New to Needs Feedback

- Assigned To set to Helmut Hummel

This is indeed a security-related option and the Security Guide is the right place for it.
I wonder which chapter of the Guide would be appropriate for this?

If you can add this in file ext_localconf.php, it is developer-related, but the Security Guide does not cover developer topics (yet). You can also put this configuration in AdditionalConfiguration.php, which means, it is not an integrator’s business, because integrators do not have access to PHP files necessarily - only administrator have - which results in chapter "Guidelines for Administrators".

Sounds a little bit weird to me, to be honest. Do you think, this is an administrator's topic? In this case, I am happy to come up with something that describes the custom HTTP headers in the BE.

By the way: I would not explain how to disable the clickjacking protection, because this decreases the level of security, which is against the idea of the Security Guide from my perspective.

#6 - 2014-03-22 14:45 - Helmut Hummel

- Status changed from Needs Feedback to Accepted

- Assigned To deleted (Helmut Hummel)

Michael Schams wrote:

> *This is indeed a security-related option and the Security Guide is the right place for it.*
> *I wonder which chapter of the Guide would be appropriate for this?*

Hm, good question, I don't know either.
This protection is like CSRF protection (which cannot really be disabled).

> *If you can add this in file ext_localconf.php, it is developer-related, but the Security Guide does not cover developer topics (yet). You can also put this configuration in AdditionalConfiguration.php, which means, it is not an integrator’s business, because integrators do not have access to PHP files necessarily - only administrator have - which results in chapter "Guidelines for Administrators".*
> *Sounds a little bit weird to me, to be honest. Do you think, this is an administrator's topic? In this case, I am happy to come up with something that describes the custom HTTP headers in the BE.*

Hm, when thinking about it, neither administrators nor integrators should change this option.

> *By the way: I would not explain how to disable the clickjacking protection, because this decreases the level of security, which is against the idea of the Security Guide from my perspective.*

Indeed. Maybe we do not need to cover this at all, since disabling this was only built in for backwards compatibility in the (rare) case when people do need to embed backend modules in iframes from different domains.
We could discuss, if we should send this header in any case in future versions, or at least add a warning in the reports module if this header is not among the header sent in the backend.

But what would fit very nicely into the Security Guide is how to protect the frontend from this attack vector.
This can either be an integrators task by setting TypoScript:

```
config.additionalHeaders = X-Frame-Options: SAMEORIGIN
```

or an server admin task, by letting the webserver send this as additional HTTP header (don't have examples for that at hand currently).

Maybe the description of this frontend related task can include a small paragraph mentioning that this header is sent in the backend by default.

#7 - 2014-03-23 12:26 - Michael Schams

- Tracker changed from Bug to Task

- Assigned To set to Michael Schams

- Target version deleted (1.0.5)

- Estimated time set to 1.00

- Remaining (hours) set to 1.0

This sounds good to me. I will write an appropriate explanation in chapters Guidelines for **Administrators** and Guidelines for **Integrators**. Integrators may want to expand their TypoScript (Helmut's example, see comment number 6):

```
config.additionalHeaders = X-Frame-Options: SAMEORIGIN
```

Administrators may want to update the webserver config. Under Apache, it should be something like (note to myself: double check):

```
<IfModule mod_headers.c>
  Header set X-Frame-Options: SAMEORIGIN
</IfModule>
```

#8 - 2014-06-23 14:07 - Michael Schams

- Target version set to 1.0.6

#9 - 2014-06-23 14:13 - Michael Schams

- Category set to Guidelines for Administrators

#10 - 2014-08-02 14:10 - Michael Schams

- File task57144-1.patch added

- % Done changed from 0 to 80

- File task57144-1.patch added

- Remaining (hours) deleted (1.0)

My suggestion:

System Administrators

> Clickjacking, also knows as *user interface (UI) redress attack* or *UI redressing*, is an attack scenario where an attacker tricks a web user into clicking on a button or following a link different from what the user believes he/she is clicking on. This attack can be typically achieved by a combination of stylesheets and iframes, where multiple transparent or opaque layers manipulate the visual appearance of a HTML page.
>
> To protect the backend of TYPO3 CMS against this attack vector, a HTTP header *X-Frame-Options* is sent, which prevents embedding backend pages in an iframe on domains different than the one used to access the backend. The X-Frame-Options header has been officially standardized as `RFC 7034 <http://tools.ietf.org/html/rfc7034>`_.
>
> System administrators should consider enabling this feature at the frontend of the TYPO3 website, too. A configuration of the Apache

web server would typically look like the following::

```
  <IfModule mod_headers.c>
    Header always append X-Frame-Options SAMEORIGIN
  </IfModule>
```

The option *SAMEORIGIN* means, that the page can only be displayed in a frame on the same origin as the page itself. Other options are *DENY* (page cannot be displayed in a frame, regardless of the site attempting to do so) and *ALLOW-FROM [uri]* (page can only be displayed in a frame on the specified origin).

Integrators

Clickjacking is an attack scenario where an attacker tricks a web user into clicking on a button or following a link different from what the user believes he/she is clicking on. Please see :ref:`administrators-furtheractions-clickjacking` for further details. It may be beneficial to include a HTTP header *X-Frame-Options* on frontend pages to protect the TYPO3 website against this attack vector. Please consult with your system administrator about pros and cons of this configuration.

The following TypoScript adds the appropriate line to the HTTP header::

```
  config.additionalHeaders = X-Frame-Options: SAMEORIGIN
```

Requires review from Security Team (Helmut?).

#11 - 2014-08-02 14:11 - Michael Schams

- Status changed from Accepted to Under Review

#12 - 2014-08-02 14:41 - Michael Schams

- Parent task set to #60744

#13 - 2014-08-02 15:04 - Helmut Hummel

perfect, thanks!

#14 - 2014-08-04 13:59 - Michael Schams

- Status changed from Under Review to Closed
- % Done changed from 80 to 100

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

Files

task57144-1.patch	4.4 kB	2014-08-02	Michael Schams