Core - Bug # 54201

Epic # 55070 (Accepted): Workpackages
Epic # 55066 (New): WP: Security enhancements

Status:	Resolved	**Priority:**	Could have
Author:	Helmut Hummel	**Category:**	
Created:	2013-12-04	**Assigned To:**	
Updated:	2014-03-21	**Due date:**	
TYPO3 Version:	6.2		
PHP Version:			
Complexity:	easy		
Is Regression:	No		
Sprint Focus:			
Subject:	Implement Clickjacking Protection		

Description

- Send X-Frame-Options headers (X-Frame-Options: SAMEORIGIN) in the backend by default
  - Find an appropriate place where to send these headers
  - Add TYPO3_CONF_VARS configuration to disable it
- Provide possibility to disable this protection if not needed/ wanted.
- Coordinate with SecurityGuide writers to mention Webserver configuration for FE (no PHP implementation for frontend requests)

JS snippet to reveal body tag only when iframe included in correct parent url is not needed, as browsers supported by TYPO3 6.2 (Chrome, Safari, FF, IE >7) have support for X-Frame-Options

Related issues:

related to Security Guide - Task # 57144: Configuration to add HTTP Headers t...	**Closed**	**2014-03-21**

Associated revisions

Revision 517efee3 - 2014-03-21 19:15 - Helmut Hummel

[SECURITY] Implement Click Jacking Protection

To protect the backend from click jacking attacks
a HTTP header needs to be sent, which prevents
embedding backend pages in an iframe on domains
different than the one used to access the backend.

All recommended browsers respect this header
and prevents the backend page to be shown in an
iframe, so we do not need to implement further
JavaScript frame busting solutions.

Resolves: #54201
Documentation: #57144
Releases: 6.2
Change-Id: Ic83cae4917bb62ff8fe8b55a947ace7dba86d223
Reviewed-on: https://review.typo3.org/28601
Reviewed-by: Christian Kuhn
Reviewed-by: Markus Klein
Tested-by: Markus Klein
Reviewed-by: Wouter Wolters

Tested-by: Wouter Wolters
Reviewed-by: Ernesto Baschny
Tested-by: Ernesto Baschny

History

#1 - 2013-12-04 18:15 - Helmut Hummel

- Project changed from Core Security to Core

#2 - 2013-12-04 18:15 - Helmut Hummel

- Target version set to 6.2.0
- Is Regression set to No

#3 - 2013-12-04 18:15 - Helmut Hummel

- Status changed from New to Accepted
- Priority changed from Should have to Could have

#4 - 2014-01-20 16:44 - Ingo Schmitt

- Parent task set to #55066

#5 - 2014-01-31 13:19 - Helmut Hummel

- Estimated time set to 12.00

Helmut Hummel wrote:

> *X-Frame-Options headers*
>
> *JS snippet to reveal body tag only when iframe included in correct parent url (find reference implementation)*

#6 - 2014-01-31 13:19 - Helmut Hummel

- Complexity set to easy

#7 - 2014-03-21 12:54 - Gerrit Code Review

- Status changed from Accepted to Under Review

Patch set 1 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/28601

#8 - 2014-03-21 18:54 - Gerrit Code Review

Patch set 2 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/28601

#9 - 2014-03-21 19:30 - Helmut Hummel

- Status changed from Under Review to Resolved
- % Done changed from 0 to 100

Applied in changeset commit:517efee327b8fc4f0203bd437eca90bdbaf5d05d.