TYPO3 Core - Bug #94786

Bug # 94787 (Closed): Tracking issue related to HTML sanitization issues

Relax behavior of HTML sanitization

2021-08-10 16:29 - Oliver Hader

Status:	Closed	**Start date:**	2021-08-10
Priority:	Should have	**Due date:**	
Assignee:	Oliver Hader	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:			
TYPO3 Version:	9	**Complexity:**	
PHP Version:		**Is Regression:**	Yes
Tags:		**Sprint Focus:**	

Description

Related to https://typo3.org/security/advisory/typo3-core-sa-2021-013

Currently property lib.parseFunc.htmlSanitize = 1 is enforced, in case the behavior has not been explicitly disabled.

The idea is to relax the behavior a bit, by target the actual use-cases:

- f:format.html view-helper (using new attribute, being enabled per default)
- RTE-related invocation of stdWrap.parseFunc (no idea yet, how to tackle)

Associated revisions

Revision 6a197e75 - 2021-08-16 11:21 - Oliver Hader

[BUGFIX] Adjust default behavior of HTML sanitization in parseFunc

As a result of TYPO3-CORE-SA-2021-013, new `htmlSanitize` behavior - when invoking `ContentObjectRenderer::parseFunc` - is enabled per default, in case it was not declared otherwise. That also happened when no processing configuration was given (or could be resolved). Without having any configuration, it was obviously not possible to disable `htmlSanitize`.

Fluid's `HtmlViewHelper` can be used with an empty `parseFuncTSPath` (e.g. `<f:format.html parseFuncTSPath="">`) - due to missing (empty) configuration, sanitization was enabled per default in `parseFunc`.

With this change, property `htmlSanitize` either needs to be enabled or disabled explicitly - otherwise deprecation logs will be generated, if not given, the fall-back behavior is inferred from new feature flag `security.frontend.htmlSanitizeParseFuncDefault`.

Invoking `ContentObjectRenderer::parseFunc` without any configuration behaves like before TYPO3-CORE-SA-2021-013 was applied - it just does not process anything.

Resolves: #94786
Releases: master, 11.3, 10.4, 9.5
Change-Id: I4aee54d712ce4758f6c9c2e64a43f80b6c076406
Reviewed-on: https://review.typo3.org/c/Packages/TYPO3.CMS/+/70404
Tested-by: core-ci <typo3@b13.com>
Tested-by: Helmut Hummel <typo3@helhum.io>
Tested-by: Benni Mack <benni@typo3.org>
Reviewed-by: Helmut Hummel <typo3@helhum.io>
Reviewed-by: Benni Mack <benni@typo3.org>

Revision eec1a2b8 - 2021-08-16 11:22 - Oliver Hader

[BUGFIX] Adjust default behavior of HTML sanitization in parseFunc

As a result of TYPO3-CORE-SA-2021-013, new `htmlSanitize` behavior - when invoking `ContentObjectRenderer::parseFunc` - is enabled per

default, in case it was not declared otherwise. That also happened
when no processing configuration was given (or could be resolved).
Without having any configuration, it was obviously not possible to
disable `htmlSanitize`.

Fluid's `HtmlViewHelper` can be used with an empty `parseFuncTSPath`
(e.g. `<f:format.html parseFuncTSPath="">`) - due to missing (empty)
configuration, sanitization was enabled per default in `parseFunc`.

With this change, property `htmlSanitize` either needs to be enabled
or disabled explicitly - otherwise deprecation logs will be generated,
if not given, the fall-back behavior is inferred from new feature flag
`security.frontend.htmlSanitizeParseFuncDefault`.

Invoking `ContentObjectRenderer::parseFunc` without any configuration
behaves like before TYPO3-CORE-SA-2021-013 was applied - it just does
not process anything.

Resolves: #94786
Releases: master, 11.3, 10.4, 9.5
Change-Id: I4aee54d712ce4758f6c9c2e64a43f80b6c076406
Reviewed-on: https://review.typo3.org/c/Packages/TYPO3.CMS/+/70612
Tested-by: core-ci <typo3@b13.com>
Tested-by: Benni Mack <benni@typo3.org>
Reviewed-by: Benni Mack <benni@typo3.org>

Revision 7f2c90e2 - 2021-08-16 11:22 - Oliver Hader

[BUGFIX] Adjust default behavior of HTML sanitization in parseFunc

As a result of TYPO3-CORE-SA-2021-013, new `htmlSanitize` behavior -
when invoking `ContentObjectRenderer::parseFunc` - is enabled per
default, in case it was not declared otherwise. That also happened
when no processing configuration was given (or could be resolved).
Without having any configuration, it was obviously not possible to
disable `htmlSanitize`.

Fluid's `HtmlViewHelper` can be used with an empty `parseFuncTSPath`
(e.g. `<f:format.html parseFuncTSPath="">`) - due to missing (empty)
configuration, sanitization was enabled per default in `parseFunc`.

With this change, property `htmlSanitize` either needs to be enabled
or disabled explicitly - otherwise deprecation logs will be generated,
if not given, the fall-back behavior is inferred from new feature flag
`security.frontend.htmlSanitizeParseFuncDefault`.

Invoking `ContentObjectRenderer::parseFunc` without any configuration
behaves like before TYPO3-CORE-SA-2021-013 was applied - it just does
not process anything.

Resolves: #94786
Releases: master, 11.3, 10.4, 9.5
Change-Id: I4aee54d712ce4758f6c9c2e64a43f80b6c076406
Reviewed-on: https://review.typo3.org/c/Packages/TYPO3.CMS/+/70537
Tested-by: Benni Mack <benni@typo3.org>
Tested-by: core-ci <typo3@b13.com>
Reviewed-by: Benni Mack <benni@typo3.org>

Revision 9d2ce55e - 2021-08-16 11:22 - Oliver Hader

[BUGFIX] Adjust default behavior of HTML sanitization in parseFunc

As a result of TYPO3-CORE-SA-2021-013, new `htmlSanitize` behavior -
when invoking `ContentObjectRenderer::parseFunc` - is enabled per
default, in case it was not declared otherwise. That also happened
when no processing configuration was given (or could be resolved).
Without having any configuration, it was obviously not possible to
disable `htmlSanitize`.

Fluid's `HtmlViewHelper` can be used with an empty `parseFuncTSPath`
(e.g. `<f:format.html parseFuncTSPath="">`) - due to missing (empty)
configuration, sanitization was enabled per default in `parseFunc`.

With this change, property `htmlSanitize` either needs to be enabled
or disabled explicitly - otherwise deprecation logs will be generated,

if not given, the fall-back behavior is inferred from new feature flag
`security.frontend.htmlSanitizeParseFuncDefault`.

Invoking `ContentObjectRenderer::parseFunc` without any configuration
behaves like before TYPO3-CORE-SA-2021-013 was applied - it just does
not process anything.

Resolves: #94786
Releases: master, 11.3, 10.4, 9.5
Change-Id: I4aee54d712ce4758f6c9c2e64a43f80b6c076406
Reviewed-on: https://review.typo3.org/c/Packages/TYPO3.CMS/+/70588
Tested-by: Benni Mack <benni@typo3.org>
Tested-by: core-ci <typo3@b13.com>
Reviewed-by: Benni Mack <benni@typo3.org>

Revision f9bdf42d - 2021-09-10 17:26 - Oliver Hader

Revert "[BUGFIX] Allow links in sys_news"

This reverts commit 2d40f74822a947c814155a71d1abe9daa8cee816.

It has been discovered that the change enforced html-sanitizer
again and contradicted recent changes in issue #94786.

Resolves: #95158
Related: #67556
Releases: master
Change-Id: Icaead77b007553cef68bec3ad23e15fe853bbc05
Reviewed-on: https://review.typo3.org/c/Packages/TYPO3.CMS/+/71021
Tested-by: core-ci <typo3@b13.com>
Tested-by: Oliver Hader <oliver.hader@typo3.org>
Reviewed-by: Christian Kuhn <lolli@schwarzbu.ch>
Reviewed-by: Oliver Hader <oliver.hader@typo3.org>

Revision 7301bcd5 - 2021-10-13 12:18 - Stefan Bürk

[BUGFIX] Prevent htmlSanitize deprecation in ContentObjectRendererTest

htmlSanatize configuration has been marked as mandatory for v12 with
corresponding deprecation message with #94786 if htmlSanatize is not
set at all.

This triggers deprecation messages in ContentObjetRendererTests which
should not trigger depcrecation messages as tests should test for
correct rendering.

This patch sets htmlSanatize option for this tests to prevent these
messages.

Resolves: #95611
Related: #94786
Releases: master
Change-Id: I3222e5df98cdc2e56a86cefd7328e2b51a352f80
Reviewed-on: https://review.typo3.org/c/Packages/TYPO3.CMS/+/71602
Tested-by: core-ci <typo3@b13.com>
Tested-by: Jochen <rothjochen@gmail.com>
Tested-by: Christian Kuhn <lolli@schwarzbu.ch>
Reviewed-by: Jochen <rothjochen@gmail.com>
Reviewed-by: Christian Kuhn <lolli@schwarzbu.ch>

History

#1 - 2021-08-10 16:30 - Oliver Hader

- Description updated

#2 - 2021-08-10 16:33 - Gerrit Code Review

- Status changed from New 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/c/Packages/TYPO3.CMS/+/70404

#3 - 2021-08-10 16:39 - Oliver Hader

- Parent task set to #94787

#4 - 2021-08-10 17:13 - 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/c/Packages/TYPO3.CMS/+/70404

#5 - 2021-08-12 20:38 - Gerrit Code Review

Patch set 3 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70404

#6 - 2021-08-12 20:46 - Gerrit Code Review

Patch set 4 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70404

#7 - 2021-08-12 20:50 - Gerrit Code Review

Patch set 5 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70404

#8 - 2021-08-13 05:55 - Gerrit Code Review

Patch set 6 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70404

#9 - 2021-08-13 07:24 - Gerrit Code Review

Patch set 7 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70404

#10 - 2021-08-13 08:36 - Gerrit Code Review

Patch set 1 for branch **10.4** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70537

#11 - 2021-08-14 06:27 - Gerrit Code Review

Patch set 2 for branch **10.4** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70537

#12 - 2021-08-14 06:45 - Gerrit Code Review

Patch set 1 for branch **9.5** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70588

#13 - 2021-08-14 06:56 - Gerrit Code Review

Patch set 3 for branch **10.4** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70537

#14 - 2021-08-14 09:10 - Gerrit Code Review

Patch set 4 for branch **10.4** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70537

#15 - 2021-08-15 15:23 - Gerrit Code 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/c/Packages/TYPO3.CMS/+/70600

#16 - 2021-08-15 15:24 - 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/c/Packages/TYPO3.CMS/+/70600

#17 - 2021-08-16 05:59 - Gerrit Code Review

Patch set 3 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70600

#18 - 2021-08-16 06:50 - Gerrit Code Review

Patch set 4 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.

It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70600

#19 - 2021-08-16 09:21 - Gerrit Code Review

Patch set 5 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70600

#20 - 2021-08-16 09:47 - Gerrit Code Review

Patch set 8 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70404

#21 - 2021-08-16 09:47 - Gerrit Code Review

Patch set 5 for branch **10.4** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70537

#22 - 2021-08-16 10:02 - Gerrit Code Review

Patch set 2 for branch **9.5** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70588

#23 - 2021-08-16 10:26 - Gerrit Code Review

Patch set 1 for branch **11.3** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70612

#24 - 2021-08-16 10:30 - Gerrit Code Review

Patch set 6 for branch **10.4** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70537

#25 - 2021-08-16 10:30 - Gerrit Code Review

Patch set 3 for branch **9.5** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/70588

#26 - 2021-08-16 11:30 - Oliver Hader

- Status changed from Under Review to Resolved

- % Done changed from 0 to 100

Applied in changeset 6a197e7524dde9823bb8cc5b6923d7e0e613c141.

#27 - 2021-10-07 07:14 - Benni Mack

- Status changed from Resolved to Closed