Frontend Rendering behavior concerning TYPO3-CORE-SA-2021-013

invocation	**TYPO3 v10.4.18**[1] (past)	**TYPO3 v10.4.19** (flaky)	**TYPO3 v10.4.20** (latest)	**comments**
`stdWrap.parseFunc` (with config, having `htmlSanitize=1`)	vulnerable to XSS, processing parseFunc	HTML sanitized, processing parseFunc	HTML sanitized, processing parseFunc	used by *Fluid Styled Content* and `lib.parseFunc` and `lib.parseFunc_RTE`
`stdWrap.parseFunc` (with configuration, without explicit *htmlSanitize*[2] setting used)	vulnerable to XSS, processing parseFunc	HTML sanitized, processing parseFunc	HTML sanitized, processing parseFunc, deprecation log entry	Common in custom HTML content rendering. Can be disabled via feature flag or `htmlSanitize = 0`
`stdWrap.parseFunc` (with config, having `htmlSanitize=0`)	vulnerable to XSS, processing parseFunc	vulnerable to XSS, processing parseFunc	vulnerable to XSS, processing parseFunc	Useful for custom HTML rendering with safe input.
`stdWrap.parseFunc` (without any configuration)	vulnerable to XSS, no further processing	HTML sanitized, no further processing	vulnerable to XSS, no further processing, deprecation log entry	no-operation, invocation of `stdWrap.parseFunc` can be removed
`<f:format.html>`	vulnerable to XSS, processing parseFunc	HTML sanitized, processing parser	HTML sanitized, processing parser	can be disabled via custom `parseFuncTSPath`
`<f:format.html parseFuncTSPath=””>`	vulnerable to XSS, no further processing	HTML sanitized, no further processing *(could not be disabled)*	vulnerable to XSS, no further processing, deprecation log entry	no operation, can be replaced by `<f:format.raw>`
`<f:format.raw>`	vulnerable to XSS, no further processing	vulnerable to XSS, no further processing	vulnerable to XSS, no further processing	expected behavior, content is taken “as is”

Colors indicate potential security implication:

- vulnerable to cross-site scripting - unexpected
- vulnerable to cross-site scripting - (probably) expected
- safe & sanitized, not vulnerable to cross-site scripting
- safe & sanitized, not vulnerable to cross-site scripting - but unexpected behavior

[1] *past*: v11.3.1, v10.4.18, v9.5.28, v8.7.41, v7.6.52; *flaky*: v11.3.2, v10.4.19, v9.5.29, v8.7.42, v7.6.53; *latest*: v11.3.3, v10.4.20, v9.5.30, v8.7.43, v7.6.54

[2] applicable after v10.4.18 only; “without explicit setting used” means, the property is not given at all