TYPO3 Core - Feature #87421

Epic # 87417 (New): Integrate proper Content Security Policy (CSP) handling

Integrate CSP reporting endpoint

2019-01-13 11:44 - Oliver Hader

Status:	Accepted	**Start date:**	2019-01-13
Priority:	Should have	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	12 LTS		
PHP Version:		**Complexity:**	
Tags:		**Sprint Focus:**	

Description

In order to monitor CSP violations or misconfigurations and according reporting endpoint has to be integrated.

Documentation:

- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/report-to
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/report-uri (deprecated, but still supported & used)

Details of mismatches shall be collected and stored in an according log, containing:

- date + time
- remote address (probably configurable concerning GDPR)
- user session related information (probably configurable concerning GDPR)
- violation event (https://www.w3.org/TR/CSP2/#firing-securitypolicyviolationevent-events)

Concerning GDPR it has to be considered that logging also might be used to analyse security incidents which makes it valuable to store additional information like IP addresses.

History

#1 - 2019-01-13 11:44 - Oliver Hader

- Assignee deleted (Oliver Hader)

#2 - 2021-11-17 21:42 - Oliver Hader

- Target version changed from Candidate for Major Version to 12 LTS

#3 - 2021-11-17 21:42 - Oliver Hader

- Status changed from New to Accepted