You'll find in tiki-admin.php?page=security

The stronger settings are activated by default in new installs of Tiki25+. For previous versions, and if upgrading from <=24 to =>25, you need to activate manually. We chose not to make this automatic because these higher security measures can cause some side-effects on highly customized Tiki instances.

Name	Description	Introduced in Tiki version
HTTP header X-Frame-Options	The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a ame>, rame> or ject>	16
HTTP Header X-XSS-Protection	The X-XSS-Protection header is designed to enable the cross-site scripting (XSS) filter built into modern web browsers	16
HTTP Header X-Content-Type-Options	The X-Content-Type-Options header is a marker used by the server to indicate that the MIME types advertised in the Content-Type headers should not be changed and be followed.	17
HTTP Header Content-Security-Policy	The Content-Security-Policy header allows web site administrators to control resources the user agent is allowed to load for a given page.	17
HTTP Header Strict-Transport-Security	The Strict-Transport-Security header (often abbreviated as HSTS) is a security feature that lets a web site tell browsers that it should only be communicated with using HTTPS, instead of using HTTP.	17
HTTP Header Public-Key-Pins	The Public-Key-Pins header associates a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates. If one or several keys are pinned and none of them are used by the server, the browser will not accept the response as legitimate, and will not display it.	17