OpenAtlas - Feature #1011

Additional security features

2019-04-07 17:08 - Alexander Watzinger

Status:	Closed	**Start date:**	2019-04-07
Priority:	Low	**Estimated time:**	8.00 hours
Assignee:	Alexander Watzinger		
Category:	Backend		
Target version:	3.16.0		

Description

To provide additional security we tested OpenAtlas at Mozilla and began implementing the suggestions:
https://observatory.mozilla.org/analyze/demo-dev.openatlas.eu

In application:

- HTTP Strict Transport Security https://infosec.mozilla.org/guidelines/web_security#http-strict-transport-security
- X-Content-Type-Options https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options
- X-Frame-Options https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
- X-XSS-Protection https://infosec.mozilla.org/guidelines/web_security#x-xss-protection

- SESSION_COOKIE_SAMESITE
- REMEMBER_COOKIE_SECURE

Documented how to activated if using HTTPS only:

- SESSION_COOKIE_SECURE: https://infosec.mozilla.org/guidelines/web_security#cookies

History

#1 - 2019-04-07 17:39 - Alexander Watzinger

- Description updated

#2 - 2019-04-07 17:47 - Alexander Watzinger

- Description updated

#3 - 2019-04-07 17:55 - Alexander Watzinger

- Description updated

#4 - 2019-04-07 17:55 - Alexander Watzinger

- Description updated

#5 - 2019-04-07 18:09 - Alexander Watzinger

- Description updated

#6 - 2019-04-11 23:41 - Alexander Watzinger

- Description updated

#7 - 2019-04-15 15:01 - Alexander Watzinger

- Status changed from In Progress to Closed

Only suggestion which was not implemented: Content Security Policy

This would need a complete rebuild of the application (no inline JavaScript or CSS) so we wait for the next major frontend upgrade.