

Plugin local_csp

Das Plugin local_csp erlaubt das Prüfen und Erzwingen von HTTP-Headern nach der "[Content Security Policy \(CSP\)](#)"

Content Security Policy (CSP)

Das Plugin ermöglicht es, das Setzen von bestimmten Headern auf einer Moodle-Instanz zu beobachten und die Auswirkungen zu sammeln. Man kann die gewünschten Header anschließend auch setzen.

Das Plugin setzt zum Prüfen den [Content-Security-Policy-Report-Only](#) Header. Dieser Header hat u.a. als Parameter einen *Endpoint*, also eine URL: in der Datei `/local/csp/collector.php` werden die Daten per POST-Request entgegengenommen und in eine Tabelle geschrieben.

Ein Scheduled Task (`cleanup_csp_task`) räumt die Tabelle nach der eingestellten Zeit wieder auf (Standard 26 Wochen: `local_csp | cleanup_duration`).

Zusätzlich zu den "[Content Security Policy \(CSP\)](#)"-Headern erlaubt das Plugin auch das Setzen von "[Feature-Policy](#)"-Headern. Hierbei handelt es sich um eine experimentelle Technologie (siehe "[Permissions Policy](#)"), mit der kontrolliert werden kann, welche Eigenschaften des Browsers eine Webseite nutzen darf.

Anzeige von Warnmeldungen

Mit der Einstellung `local_csp | notifications_enable_reported` werden gelbe Kästchen auf jeder Webseite eingeblendet, die über die potentiellen Auswirkungen der aktuell gesetzten Header informieren.

Die Anzeige dieser Warnmeldungen ist an die Capability `local/csp:seenotifications` geknüpft, die standardmäßig für die Rollen *teacher*, *editingteacher* und *manager* gesetzt ist.

Docker moodle405

Potentially insecure content reported!

This page contains embedded content that the administrators consider potentially insecure.

Content from the following sources was reported to the administrators:

- [http://localhost:8405/lib/ajax/service-nologin.php?
info=core_output_load_template_with_dependencies&cachekey=1785328873&args=%5B%7B%22index%22%3A%7B%7D%7D%5D](http://localhost:8405/lib/ajax/service-nologin.php?info=core_output_load_template_with_dependencies&cachekey=1785328873&args=%5B%7B%22index%22%3A%7B%7D%7D%5D)

Potentially insecure content reported!

This page contains embedded content that the administrators consider potentially insecure.

Content from the following sources was reported to the administrators:

- http://localhost:8405/theme/yui_combo.php?rollup/3.18.1/yui-moodlesimple.css
- http://localhost:8405/theme/styles.php/boost/1785328872_1785319271/all
- http://localhost:8405/theme/font.php/boost/core/1785328870/fa-regular-400.woff2
- http://localhost:8405/theme/font.php/boost/core/1785328870/fa-regular-400.ttf
- http://localhost:8405/theme/font.php/boost/core/1785328870/fa-solid-900.woff2
- http://localhost:8405/theme/font.php/boost/core/1785328870/fa-solid-900.ttf
- http://localhost:8405/theme/font.php/boost/core/1785328870/fa-brands-400.woff2
- http://localhost:8405/theme/font.php/boost/core/1785328870/fa-brands-400.ttf
- http://localhost:8405/theme/image.php/boost/theme/1785328872/favicon
- https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured
- http://localhost:8405/theme/font.php/boost/core/1785328870/fa-solid-900.woff2
- http://localhost:8405/lib/ajax/service-nologin.php?
info=core_output_load_template_with_dependencies&cachekey=1785328873&args=%5B%7B%22index%22%
info=core_output_load_template_with_dependencies,core_output_load_template_with_dependencies,core_o

Available courses

Report

Wie oben erwähnt sammelt das Plugin über den *Endpoint* des Headers alle Daten in einer Tabelle. Deren Inhalt kann man sich über den "CSP violation report" ansehen:

CSP violation reports

Reset all statistics

Download table data as

Comma separated values (.csv)

Download

#	Policy	Domain	Blocked paths	Top Violation Sources	Courses	Last	Action
109	font-src	localhost	theme/font.php/boost/core/1785318548/... ⁽¹⁹⁾ theme/font.php/boost/core/1785318548/... ⁽¹⁰⁾ theme/font.php/boost/core/1785318548/... ⁽¹⁰⁾	admin/settings.php?section=local_csp_... ⁽³⁵⁾ local/csp/csp_report.php ⁽²¹⁾ ?redirect=0 ⁽²⁰⁾	docker_moodle405 ⁽¹⁰⁹⁾	30/07/26, 07:38 4 secs	Reset
87	connect-src	localhost	lib/ajax/service-nologin.php?info=cor... ⁽¹²⁾ lib/ajax/service-nologin.php?info=cor... ⁽¹⁰⁾ lib/ajax/service-nologin.php?info=cor... ⁽⁸⁾	admin/settings.php?section=local_csp_... ⁽¹⁹⁾ my/ ⁽¹⁸⁾ admin/search.php ⁽¹³⁾	docker_moodle405 ⁽⁸⁷⁾	30/07/26, 07:33 4 mins 15 secs	Reset
48	style-src-elem	localhost	theme/yui_combo.php?rollup%2F3_18_1%2... ⁽²⁴⁾ theme/styles.php/boost/1785318548_178... ⁽¹⁴⁾ theme/styles.php/boost/1785328872_178... ⁽¹⁰⁾	admin/settings.php?section=local_csp_... ⁽¹²⁾ admin/search.php ⁽⁸⁾ local/csp/csp_report.php ⁽⁸⁾	docker_moodle405 ⁽⁴⁸⁾	30/07/26, 07:33 4 mins 32 secs	Reset
33	img-src	localhost	theme/image.php/boost/theme/178531854... ⁽¹⁶⁾ theme/image.php/boost/theme/178532887... ⁽¹¹⁾ theme/image.php/boost/block_timeline/... ⁽²⁾	my/ ⁽⁸⁾ admin/settings.php?section=local_csp_... ⁽⁶⁾ admin/search.php ⁽⁴⁾	docker_moodle405 ⁽³³⁾	30/07/26, 07:33 4 mins 32 secs	Reset
24	script-src-elem	cdn.jsdelivr.net	npm/mathjax@2.7.9/MathJax.js?delaySta... ⁽²⁴⁾	admin/settings.php?section=local_csp_... ⁽⁶⁾ admin/search.php ⁽⁴⁾ local/csp/csp_report.php ⁽⁴⁾	docker_moodle405 ⁽²⁴⁾	30/07/26, 07:33 4 mins 41 secs	Reset
4	default-src	localhost	lib/javascript.php/1785318549/lib/req... ⁽²⁾ ?redirect=0 ⁽¹⁾ admin/settings.php?section=local_csp_... ⁽¹⁾	?redirect=0 ⁽²⁾ admin/settings.php?section=local_csp_... ⁽²⁾	docker_moodle405 ⁽⁴⁾	29/07/26, 13:19 18 hours 18 mins	Reset
1	frame-src	localhost	local/csp/samples/sample.html ⁽¹⁾	local/csp/mixed_content_examples.php ⁽¹⁾	docker_moodle405 ⁽¹⁾	29/07/26, 13:05 18 hours 32 mins	Reset
1	script-src-elem	code.jquery.com	jquery-3.5.1.min.js ⁽¹⁾	local/csp/mixed_content_examples.php ⁽¹⁾	docker_moodle405 ⁽¹⁾	29/07/26, 13:05 18 hours 32 mins	Reset

Einstellungen

Mit der Einstellung `local_csp | csp_header_enable` aktiviert man das Reporting.

Folgende Direktiven schlägt das Plugin standardmäßig vor:

- `default-src https;;`
- `script-src 'self' 'unsafe-inline' 'unsafe-eval';`
- `font-src https: data;;`
- `style-src https: 'unsafe-inline';`
- `img-src https: data;;`

Configure CSP header

CSP works through adding a special HTTP response header to every Moodle page. Modern browsers, when they see this header, are able to perform certain actions e.g. block insecure content on such pages. Please read more about CSP [here](#).

If you leave any of these settings blank CSP headers will not be used.

CSP header enable local_csp csp_header_enable	☒ Default: No
Tick this checkbox to enable CSP headers	
Content-Security-Policy-Report-Only local_csp csp_header_reporting	<code>default-src https; script-src 'self' 'unsafe-inline' 'unsafe-eval'; font-src https: data; style-src https: 'unsafe-inline'; img-src https: data;</code> Default: default-src https;; script-src 'self' 'unsafe-inline' 'unsafe-eval'; font-src https: data;; style-src https: 'unsafe-inline'; img-src https: data;; Monitor and report CSP violations
Notify when reporting local_csp notifications_enable_reported	☒ Default: No
Display a notification to the user, when the Report-Only-CSP is triggered on the visited page, listing the URIs in question.	
Content-Security-Policy local_csp csp_header_enforcing	Default: Empty Enforce browsers to follow CSP directives, e.g. block loading insecure content
Notify when enforcing local_csp notifications_enable_enforced	☐ Default: No
Display a notification to the user, when the CSP is enforced on the visited page, listing all the blocked URIs on that page.	
Enable Feature-Policy header local_csp feature_policy_enable	☐ Default: No
Send a feature policy header as part of the Plugin headers sent. This header controls what browser features are allowed to be accessed by DOM elements.	
Feature-Policy local_csp feature_policy	Default: Empty Enter the feature policy to be sent. Add one entry per line, ending with a semicolon. E.g. microphone 'none';
CSP cleanup duration local_csp cleanup_duration	26 weeks Default: 26 weeks Removes CSP records that have not had any violations during the selected time period. The counts of records that have had violations will not be reset. Setting the expiry to 0 will remove all records. Save changes

Links / Quellen

<https://marketplace.moodle.com/plugins/1506>

https://github.com/catalyst/moodle-local_csp

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP>

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Content-Security-Policy-Report-Only>

<https://moodle.org/mod/forum/discuss.php?d=460784> - hier gibt es einen Vorschlag für ein Set an Headern

Autorin: [Melanie Treitinger](#), Ruhr-Universität Bochum

Version #3

Erstellt: 2026-07-29 14:13:36 UTC von Melanie Treitinger

Zuletzt aktualisiert: 2026-07-30 07:21:35 UTC von Melanie Treitinger