Security Report Summary



Site:	https://demo.cofys.de
IP Address:	152.53.134.209
Report Time:	25 Oct 2026 15:29:30 UTC
Headers:	✔ Content-Security-Policy ✔ Permissions-Policy ✔ Referrer-Policy ✔ Strict-Transport-Security ✔ X-Content-Type-Options ✔ X-Frame-Options

Raw Headers

HTTP/2	200
alt-svc	h3=":443"; ma=2592000
cache-control	max-age=0, must-revalidate, private
content-encoding	gzip
content-security-policy	**default-src** 'self'; **script-src** 'self' *.cofys.de *.ucdn.de; **style-src** 'self' 'unsafe-inline' *.cofys.de; **object-src** 'none'; **base-uri** 'self'; **connect-src** 'self' *.mapbox.com *.cofys.de *.ucdn.de; **font-src** 'self' data: *.cofys.de *.ucdn.de; **frame-src** 'self' https://www.youtube-nocookie.com https://www.youtube.com; **img-src** * blob: data:; **manifest-src** 'self'; **media-src** 'self'; **worker-src** 'self' blob:; **form-action** 'self' https://checkout.stripe.com https://www.paypal.com https://www.sandbox.paypal.com; **frame-ancestors** 'self'; **upgrade-insecure-requests**;
content-type	text/html; charset=UTF-8
date	Sun, 25 Oct 2026 15:29:30 GMT
expires	Sun, 25 Oct 2026 15:29:30 GMT
permissions-policy	**autoplay**=(self), **camera**=(self), **encrypted-media**=(self), **fullscreen**=(self), **geolocation**=(self), **microphone**=(self), **midi**=(self), **payment**=(self)
referrer-policy	**strict-origin-when-cross-origin**
server	FrankenPHP Caddy
set-cookie	SESSION_v18=f29639e69aa8a15b1281065eed7aba48; expires=Sun, 25 Oct 2026 16:29:30 GMT; Max-Age=3600; path=/; **secure**; **httponly**; samesite=lax
strict-transport-security	**max-age**=63072000; **includeSubDomains**; **preload**
vary	Accept-Encoding
x-content-type-options	**nosniff**
x-frame-options	**SAMEORIGIN**

x-powered-by	PHP/8.5.12
x-xss-protection	**1**; **mode**=block

Upcoming Headers

Cross-Origin-Embedder-Policy	Cross-Origin Embedder Policy allows a site to prevent assets being loaded that do not grant permission to load them via CORS or CORP.
Cross-Origin-Opener-Policy	Cross-Origin Opener Policy allows a site to opt-in to Cross-Origin Isolation in the browser.
Cross-Origin-Resource-Policy	Cross-Origin Resource Policy allows a resource owner to specify who can load the resource.

Additional Information

content-security-policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets. Analyse this policy in more detail. You can sign up for a free account on Report URI to collect reports about problems on your site.
permissions-policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.
referrer-policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
server	This Server header seems to advertise the software being run on the server but you can remove or change this value.
set-cookie	There is no Cookie Prefix on this cookie.
strict-transport-security	HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS.
x-content-type-options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
x-frame-options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking.
x-powered-by	X-Powered-By can usually be seen with values like "PHP/5.5.9-1ubuntu4.5" or "ASP.NET". Trying to minimise the amount of information you give out about your server is a good idea. This header should be removed or the value changed.
x-xss-protection	X-XSS-Protection sets the configuration for the XSS Auditor built into older browsers. The recommended value was "X-XSS-Protection: 1; mode=block" but you should now look at Content Security Policy instead.