Security Report Summary

A

Site:	https://demo.cofys.de/forum/forums/
IP Address:	185.232.70.247
Report Time:	19 Jan 2022 14:34:12 UTC
Headers:	✔ Strict-Transport-Security ✔ X-Frame-Options ✔ X-Content-Type-Options ✔ Referrer-Policy ✔ Permissions-Policy ✔ Content-Security-Policy
Warning:	Grade capped at A, please see warnings below.

Raw Headers

HTTP/1.1	200 OK
Server	nginx/1.18.0 (Ubuntu)
Date	Wed, 19 Jan 2022 14:34:11 GMT
Content-Type	text/html; charset=UTF-8
Transfer-Encoding	chunked
Connection	keep-alive
Expires	Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control	no-store, no-cache, must-revalidate
Pragma	no-cache
Set-Cookie	**__Secure-**PHPSESSID_v2=41n0h9b9jqlsuk91e9of9gjan0; path=/; **secure**; **HttpOnly**; **SameSite**=Strict
Vary	Accept-Encoding
Strict-Transport-Security	**max-age**=63072000; **includeSubDomains**
X-Frame-Options	**SAMEORIGIN**
X-Content-Type-Options	**nosniff**
X-XSS-Protection	**1**; **mode**=block
Expect-CT	: **max-age**=86400, **enforce**
Referrer-Policy	**strict-origin**
Permissions-Policy	**autoplay**=(self), **camera**=(self), **document-domain**=(self), **encrypted-media**=(self), **fullscreen**=(self), **geolocation**=(self), **microphone**=(self), **midi**=(self), **payment**=(self)
Content-Security-Policy	**default-src** *'self'*; **script-src** *'self'* *.trueforce.ca *.ucdn.de *.cofys.de https://www.google.com/recaptcha/ *.gstatic.com; **style-src** *'self' 'unsafe-inline'* *.trueforce.ca *.ucdn.de *.cofys.de https://fonts.googleapis.com; **object-src** *'self'*; **base-uri** *'self'*; **connect-src** *.trueforce.ca *.mapbox.com *.ucdn.de *.cofys.de *.datatables.net *.googleapis.com *.gstatic.com *.google.com *'self'*; **font-src** *'self'* *.trueforce.ca *.ucdn.de *.cofys.de *.gstatic.com; **frame-src** *'self'* https://www.google.com https://www.youtube-nocookie.com https://www.youtube.com; **img-src** * blob: data: *.trueforce.ca *.ucdn.de *.cofys.de; **manifest-src** *'self'*; **media-src** *'self'*; **worker-src** *'self'* blob:; **form-action** *; **frame-ancestors** *'self'*;

Warnings

Content-Security-Policy	This policy contains 'unsafe-inline' which is dangerous in the style-src directive.

Additional Information

Server	This Server header seems to advertise the software being run on the server but you can remove or change this value.
Set-Cookie	This cookie has the appropriate flags set.
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-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-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-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.
Expect-CT	Expect-CT allows a site to determine if they are ready for the upcoming Chrome requirements and/or enforce their CT policy.
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.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.
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.