Scan Summary

Host:	demo.cofys.de
Scan ID #:	23983900
Start Time:	January 19, 2022 3:46 PM
Duration:	9 seconds
Score:	115/100
Tests Passed:	11/11

Test Scores

Test	Pass	Score	Reason
Content Security Policy	✔	0	Content Security Policy (CSP) implemented with unsafe sources inside `style-src`. This includes `'unsafe-inline'`, `data:` or overly broad sources such as https:.
Cookies	✔	+5	All cookies use the `Secure` flag, session cookies use the `HttpOnly` flag, and cross-origin restrictions are in place via the `SameSite` flag
Cross-origin Resource Sharing	✔	0	Content is not visible via cross-origin resource sharing (CORS) files or headers
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)
HTTP Strict Transport Security	✔	0	HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000)
Redirection	✔	0	Initial redirection is to HTTPS on same host, final destination is HTTPS
Referrer Policy	✔	+5	Referrer-Policy header set to `"no-referrer"`, `"same-origin"`, `"strict-origin"` or `"strict-origin-when-cross-origin"`
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin
X-Content-Type-Options	✔	0	X-Content-Type-Options header set to `"nosniff"`
X-Frame-Options	✔	+5	X-Frame-Options (XFO) implemented via the CSP `frame-ancestors` directive
X-XSS-Protection	✔	0	X-XSS-Protection header set to `"1; mode=block"`

Content Security Policy Analysis

Test	Pass
Blocks execution of inline JavaScript by not allowing `'unsafe-inline'` inside `script-src`	✓
Blocks execution of JavaScript's `eval()` function by not allowing `'unsafe-eval'` inside `script-src`	✓
Blocks execution of plug-ins, using `object-src` restrictions	✓
Blocks inline styles by not allowing `'unsafe-inline'` inside `style-src`	✗
Blocks loading of active content over HTTP or FTP	✓
Blocks loading of passive content over HTTP or FTP	✓
Clickjacking protection, using `frame-ancestors`	✓
Deny by default, using `default-src 'none'`	✗
Restricts use of the `<base>` tag by using `base-uri 'none'`, `base-uri 'self'`, or specific origins	✓
Restricts where `<form>` contents may be submitted by using `form-action 'none'`, `form-action 'self'`, or specific URIs	✗
Uses CSP3's `'strict-dynamic'` directive to allow dynamic script loading (optional)	–

Cookies

Name	Expires	Path	Secure ()	HttpOnly ()	SameSite ()	Prefixed ()
__Secure-PHPSESSID_v2	Session	/	✓	✓	Strict	✓

Grade History

Date	Score	Grade
October 5, 2021 12:00 PM	115	A+

Raw Server Headers

Header	Value
Cache-Control:	no-store, no-cache, must-revalidate
Connection:	keep-alive
Content-Encoding:	gzip
Content-Length:	2725

Header	Value
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';
Content-Type:	text/html; charset=UTF-8
Date:	Wed, 19 Jan 2022 14:46:11 GMT
Expect-CT:	: max-age=86400, enforce
Expires:	Thu, 19 Nov 1981 08:52:00 GMT
Permissions-Policy:	autoplay=(self), camera=(self), document-domain=(self), encrypted-media=(self), fullscreen=(self), geolocation=(self), microphone=(self), midi=(self), payment=(self)
Pragma:	no-cache
Referrer-Policy:	strict-origin
Server:	nginx/1.18.0 (Ubuntu)
Strict-Transport-Security:	max-age=63072000; includeSubDomains
Vary:	Accept-Encoding
X-Content-Type-Options:	nosniff
X-Frame-Options:	SAMEORIGIN
X-XSS-Protection:	1; mode=block