# HTTP Observatory Report

Report Feedback

## Scan summary: demo.cofys.de

A+

Score: 110 / 100
Scan Time: 2 minutes ago
Tests Passed: 11 / 12

## Scan results

## Scoring

| Test | Score | Reason | Recommendation |
|---|---|---|---|
| Content Security Policy (CSP) | 0 ✓ | Content Security Policy (CSP) implemented with unsafe sources inside style-src. This includes **'unsafe-inline'**, **data:** or overly broad sources such as **https**. **'form-action'** is set to **'self'**, **'none'** or **'specific source'** | Lock down **style-src** directive, removing **'unsafe-inline'**, **data:** and broad sources. |
| 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. | None |
| Cross Origin Resource Sharing (CORS) | 0 ✓ | Content is not visible via cross-origin resource sharing (CORS) files or headers. | None |

| Test | Score | Reason | Recommendation |
| --- | --- | --- | --- |
| Redirection | 0 ✓ | Initial redirection is to HTTPS on same host, final destination is HTTPS | None |
| Referrer Policy | +5 ✓ | **`Referrer-Policy`** header set to **`no-referrer`**, **`same-origin`**, **`strict-origin`** or **`strict-origin-when-cross-origin`**. | None |
| Strict Transport Security (HSTS) | 0 ✓ | **`Strict-Transport-Security`** header set to a minimum of six months (`15768000`). | Consider preloading: this requires adding the **`preload`** and **`includeSubDomains`** directives and setting **`max-age`** to at least **`31536000`** (1 year), and submitting your site to https://hstspreload.org/. |
| Subresource Integrity | −5 ✗ | Subresource Integrity (SRI) not implemented, but all external scripts are loaded over HTTPS. | Add SRI to external scripts. |
| X-Content-Type-Options | 0 ✓ | **`X-Content-Type-Options`** header set to **`nosniff`**. | None |
| X-Frame-Options | +5 ✓ | **`X-Frame-Options`** (XFO) implemented via the CSP frame-ancestors directive. | None |
| Cross Origin Embedder Policy | 0 ✓ | **`Cross-Origin-Embedder-Policy`** header not implemented. | Set to **`require-corp`** or **`credentialless`**. |
| Cross Origin Opener Policy | 0 ✓ | **`Cross-Origin-Opener-Policy`** header not implemented. | Set to **`same-origin`**, **`same-origin-allow-popups`**, or **`noopener-allow-popups`**. |
| Cross Origin Resource Policy | - | Cross Origin Resource Policy (CORP) is not implemented (defaults to **`cross-origin`**). | None |

# CSP analysis

✓ Content Security Policy (CSP) implemented with unsafe sources inside style-src. This includes `'unsafe-inline'`, `data:` or overly broad sources such as `https`. `'form-action'` is set to `'self'`, `'none'` or `'specific source'`

| Test | Result | Info |
| --- | --- | --- |
| Blocks execution of inline JavaScript by not allowing `'unsafe-inline'` inside `script-src` | ✓ | Blocking the execution of inline JavaScript provides CSP's strongest protection against cross-site scripting attacks. Moving JavaScript to external files can also help make your site more maintainable. |
| Blocks execution of JavaScript's `eval()` function by not allowing `'unsafe-eval'` inside `script-src` | ✓ | Blocking the use of JavaScript's `eval()` function can help prevent the execution of untrusted code. |
| Blocks execution of plug-ins, using `object-src` restrictions | ✓ | Blocking the execution of plug-ins via `object-src 'none'` or as inherited from `default-src` can prevent attackers from loading Flash or Java in the context of your page. |
| Blocks inline styles by not allowing `'unsafe-inline'` inside `style-src` | ✗ | Blocking inline styles can help prevent attackers from modifying the contents or appearance of your page. Moving styles to external stylesheets can also help make your site more maintainable. |
| Blocks loading of active content over HTTP or FTP | ✓ | Loading JavaScript or plugins can allow a man-in-the-middle to execute arbitrary code or your website. Restricting your policy and changing links to HTTPS can help prevent this. |
| Blocks loading of passive content over HTTP or FTP | ✓ | This site's Content Security Policy allows the loading of passive content such as images or videos over insecure protocols such as HTTP or FTP. Consider changing them to load them over HTTPS. |
| Clickjacking protection, using `frame-ancestors` | ✓ | The use of CSP's `frame-ancestors` directive offers fine-grained control over who can frame your site. |
| Deny by default, using `default-src 'none'` | ✗ | Denying by default using `default-src 'none'` can ensure that your Content Security Policy doesn't allow the loading of resources you didn't intend to allow. |
| Restricts use of the `<base>` tag by using `base-uri 'none'`, `base-uri 'self'`, or specific origins. | ✓ | The `<base>` tag can be used to trick your site into loading scripts from untrusted origins. |

| Test | Result | Info |
| --- | --- | --- |
| Restricts where `<form>` contents may be submitted by using `form-action 'none'`, `form-action 'self'`, or specific URIs | ✓ | Malicious JavaScript or content injection could modify where sensitive form data is submitted to or create additional forms for data exfiltration. |
| Uses CSP3's `'strict-dynamic'` directive to allow dynamic script loading (optional) | - | `'strict-dynamic'` lets you use a JavaScript shim loader to load all your site's JavaScript dynamically, without having to track `script-src` origins. |

# Cookies

✓ All cookies use the **`Secure`** flag, session cookies use the **`HttpOnly`** flag, and cross-origin restrictions are in place via the **`SameSite`** flag.

| Name | Expires | Path | Secure | HttpOnly | SameSite | Prefix |
| --- | --- | --- | --- | --- | --- | --- |
| SESSION_v18 | **`2026-10-25 16:33:07 UTC`** (in 58 minutes) | **`/`** | ✓ | ✓ | **`Lax`** | - |

# Raw server headers

| Header | Value |
| --- | --- |
| Date | Sun, 25 Oct 2026 15:33:07 GMT |
| Vary | Accept-Encoding |
| Server | FrankenPHP Caddy |
| Alt-Svc | h3=":443"; ma=2592000 |
| Expires | Sun, 25 Oct 2026 15:33:07 GMT |
| Connection | close |

| Header | Value |
| --- | --- |
| Set-Cookie | SESSION_v18=b0d14aaa01c38252568f9a5e11e744db; expires=Sun, 25 Oct 2026 16:33:07 GMT; Max-Age=3600; path=/; secure; httponly; samesite=lax |
| Content-Type | text/html; charset=UTF-8 |
| X-Powered-By | PHP/8.5.12 |
| Cache-Control | max-age=0, must-revalidate, private |
| Referrer-Policy | strict-origin-when-cross-origin |
| X-Frame-Options | SAMEORIGIN |
| X-Xss-Protection | 1; mode=block |
| Transfer-Encoding | chunked |
| Permissions-Policy | autoplay=(self), camera=(self), encrypted-media=(self), fullscreen=(self), geolocation=(self), microphone=(self), midi=(self), payment=(self) |
| X-Content-Type-Options | nosniff |
| 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; |
| Strict-Transport-Security | max-age=63072000; includeSubDomains; preload |

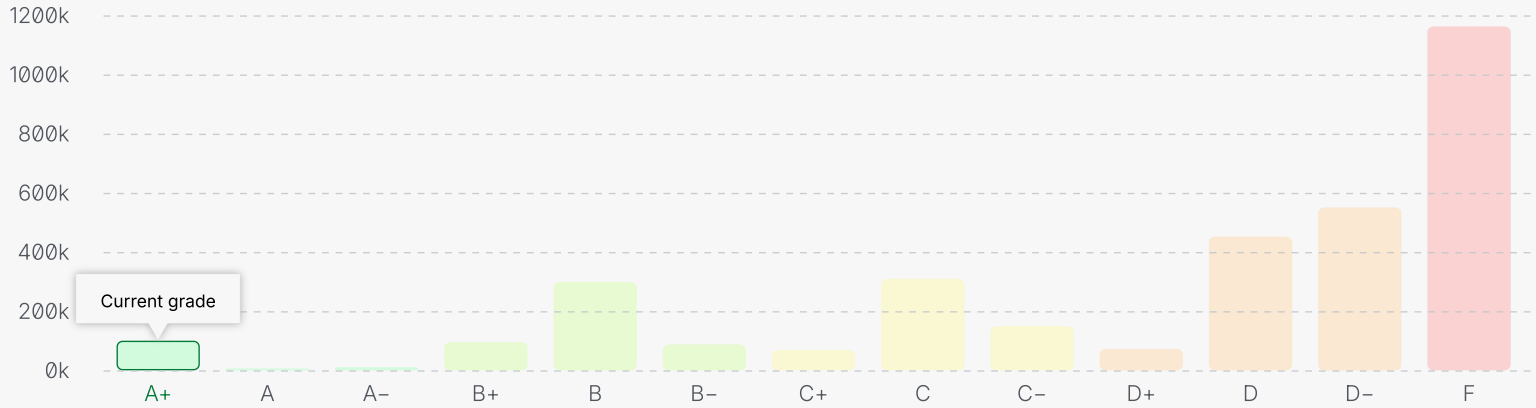
## Scan history

## Changes in score over time

| Date | Score | Grade |
| --- | --- | --- |
| Oct 25, 2026, 4:33:07 PM | 110 | A+ |

## Benchmark comparison

## Performance trends from the past year




Refer to this graph to assess the website's current status. By following the recommendations provided and rescanning, you can expect an improvement in the website's grade.

mdn_

Your blueprint for a better internet.