**Opdracht 4a SOP/CORS/CSP**

1. vraag over SOP

Geef antwoord op deze vraag. Een webpagina op de site web.nl bevat dit html-formulier. Kan deze data verstuurd worden?

    <form action="https://example.com/results.json">

        <label for="email">Enter your email: </label>

        <input type="email" name="email" required>

        <button type="submit">Subscribe</button>

    </form>

Antwoord: Ja, formulierdata kun je zenden naar een cross-origin url, zoals vermeld in de action-attribuut van het <form>

1. vraag over SOP

Geef antwoord op deze vraag. Een webpagina op de site web.nl bevat dit iframe. Is dit toegestaan? Waarom?

<iframe src="https://voorbeeld.nl/pagina.html" alt="VB iframe"></iframe>

Antwoord: Cross-origin iframes zijn toegestaan tenzij de origin (voorbeeld.nl) in de HTTP-header de X-Frame-Options op deny of sameorigin heeft ingesteld

**INLEVEROPDRACHT:**

Kijk naar deze websites. Wat is de CORS instelling (access-control-allow-origin) en wat de Content-Security-Policy. Deze kun je vinden met DevTools, tabblad Network.

Vul de tabel in en lever in op itslearning.

|  |  |  |
| --- | --- | --- |
| Site | CORS | CSP |
| belastingdienst.nl | X | |  |  | | --- | --- | | Content-Security-Policy | default-src [https://\*.belastingdienst.nl](https://*.belastingdienst.nl) <https://vinden.belastingdienst.nl> [https://\*.readspeaker.com](https://*.readspeaker.com); connect-src 'self' [https://\*.belastingdienst.nl](https://*.belastingdienst.nl) [https://\*.optimizely.com](https://*.optimizely.com) [https://\*.readspeaker.com](https://*.readspeaker.com) \*.abtasty.com; child-src 'self' <https://belastingdienst.nl> [https://\*.belastingdienst.nl](https://*.belastingdienst.nl) [https://\*.cdn.optimizely.com](https://*.cdn.optimizely.com) <https://secure.opinionlab.com> [https://\*.readspeaker.com](https://*.readspeaker.com) <https://www.anbi-instellingen.nl> <https://www.youtube.com> <https://www.youtube-nocookie.com>; frame-src 'self' [https://\*.belastingdienst.nl](https://*.belastingdienst.nl) [h…](https://*.readspeaker.com)'self' <https://n01d05.cumulus-cloud.com> [https://\*.readspeaker.com](https://*.readspeaker.com) <https://img.youtube.com> data: [https://\*.belastingdienst.nl](https://*.belastingdienst.nl) blob: data: \*.abtasty.com; font-src 'self' [https://\*.belastingdienst.nl](https://*.belastingdienst.nl) blob: data: \*.abtasty.com; script-src 'self' [https://\*.belastingdienst.nl](https://*.belastingdienst.nl) <https://cdn.optimizely.com> [https://\*.readspeaker.com](https://*.readspeaker.com) <https://bdtm.containers.piwik.pro> 'unsafe-eval' 'unsafe-inline' blob: \*.abtasty.com ; style-src 'self' [https://\*.belastingdienst.nl](https://*.belastingdienst.nl) [https://\*.readspeaker.com](https://*.readspeaker.com) \*.abtasty.com 'unsafe-inline' | |
| knmi.nl | X | X |
| summacollege.nl | X | X |
| w3schools.com | X | |  |  | | --- | --- | | content-security-policy | frame-ancestors 'self' <https://mycourses.w3schools.com>; | |
| rijdendetreinen.nl/feed.json | X | X |
| api.open-notify.org/iss-now.json | \* | X |