Generado: 30/03/2026 02:48:08

50%

Riesgo Medio

URL Analizada: `https://www.global66.com/cl`

9

Headers Analizados

5

Presentes

4

Faltantes

Headers Presentes (5)

X-Frame-Options Presente

Previene ataques de clickjacking al controlar si la página puede ser embebida en iframes.

Valor: SAMEORIGIN

X-Content-Type-Options Presente

Evita que el navegador interprete archivos como un tipo MIME diferente al declarado (MIME sniffing).

Valor: nosniff

Referrer-Policy Presente

Controla cuánta información del referrer se envía en las peticiones. Protege la privacidad del usuario.

Valor: `same-origin`

Permissions-Policy (Feature-Policy) Presente

Controla qué APIs del navegador puede usar la página (geolocalización, cámara, micrófono, etc.).

Valor:
`accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-write=(),geolocation=(),gyroscope=(),hi`

COEP (Cross-Origin Embedder Policy) Presente

Previene la carga de recursos cross-origin que no otorguen permiso explícito.

Valor: `require-corp`

Headers Faltantes (4)

HSTS (HTTP Strict Transport Security) Faltante Critico

Fuerza a los navegadores a usar HTTPS exclusivamente, protegiendo contra ataques de downgrade y secuestro de cookies.

Recomendacion: max-age=31536000; includeSubDomains; preload

CSP (Content Security Policy) Faltante Critico

Define qué recursos pueden cargarse en la página. Es la defensa más efectiva contra ataques XSS y de inyección de datos.

Recomendacion: default-src 'self'; script-src 'self'; style-src 'self' 'unsafe-inline'

X-XSS-Protection Faltante Bajo

Activa el filtro XSS integrado en navegadores antiguos. Aunque obsoleto, proporciona protección adicional.

Recomendacion: 1; mode=block

X-Permitted-Cross-Domain-Policies Faltante Bajo

Controla cómo Adobe Flash y PDF pueden acceder a datos del sitio.

Recomendacion: none