Generado: 13/05/2026 20:45:09

75%

Riesgo Medio

URL Analizada: `https://www.tvn.cl/`

9

Headers Analizados

7

Presentes

2

Faltantes

Headers Presentes (7)

CSP (Content Security Policy) Presente

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

Valor: `default-src * data: blob: about: ws: wss: 'unsafe-inline' 'unsafe-eval';`

X-Frame-Options Presente

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

Valor: `no-referrer-when-downgrade`

X-Content-Type-Options Presente

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

Valor: `nosniff`

X-XSS-Protection Presente

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

Valor: `1`

Referrer-Policy Presente

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

Valor: `no-referrer-when-downgrade`

Permissions-Policy (Feature-Policy) Presente

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

Valor: `browsing-topics=()`

X-Permitted-Cross-Domain-Policies Presente

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

Valor: `none`

Headers Faltantes (2)

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

COEP (Cross-Origin Embedder Policy) Faltante Bajo

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

Recomendacion: require-corp