Generado: 17/03/2026 12:03:53

80%

Riesgo Bajo

URL Analizada: `https://www.youtube.com/watch?v=ZGPOC3cHHW0`

9

Headers Analizados

6

Presentes

3

Faltantes

Headers Presentes (6)

HSTS (HTTP Strict Transport Security) Presente

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

Valor: `max-age=31536000`

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: `require-trusted-types-for 'script'`

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`

X-XSS-Protection Presente

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

Valor: `0`

Permissions-Policy (Feature-Policy) Presente

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

Valor: `ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-wow64=*, ch-ua-form-factors=*, ch-ua-platform=*, ch-ua-platform-version=*`

Headers Faltantes (3)

Referrer-Policy Faltante Medio

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

Recomendacion: strict-origin-when-cross-origin

X-Permitted-Cross-Domain-Policies Faltante Bajo

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

Recomendacion: none

COEP (Cross-Origin Embedder Policy) Faltante Bajo

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

Recomendacion: require-corp