

45%

Riesgo Alto

URL Analizada: <https://www.compunetgroup.net/>

9

Headers Analizados

3

Presentes

6

Faltantes

Headers Presentes (3)

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=64072000; includeSubDomains; preload

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

Headers Faltantes (6)

CSP (Content Security Policy) **Faltante** Crítico

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

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

Permissions-Policy (Feature-Policy) **Faltante** Medio

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

Recomendacion: geolocation=(), microphone=(), camera=()

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