Generado: 22/01/2026 21:49:45

80%

Riesgo Bajo

URL Analizada: `https://facebook.com`
URL Final: `https://web.facebook.com/?_rdc=1&_rdr`

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=15552000; preload
```

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 blob: 'self' https://*.fbsbx.com *.facebook.com *.fbcdn.net;script-src
*.facebook.com *.fbcdn.net *.facebook.net 127.0.0.1:* 'nonce-52hTAmWU' blob: 'self'
connect.facebook.net 'unsafe-eval' https://*.google-analytics.com *.google.com;style-src *.fbcdn.net
data: *.facebook.com 'unsafe-inline' https://fonts.googleapis.com;connect-src *.facebook.com
facebook.com *.fbcdn.net *.facebook.net wss://*.facebook.com:* wss://*.whatsapp.com:*
```

```
wss://*.fbcdn.net attachment.fbsbx.com ws://localhost:* blob: *.cdninstagram.com 'self'
http://localhost:3103 wss://gateway.facebook.com wss://edge-chat.facebook.com
wss://snaptu-d.facebook.com wss://kaios-d.facebook.com/ v.whatsapp.net *.fbsbx.com *.fb.com
*.instagram.com https://*.google-analytics.com;font-src data: *.facebook.com *.fbcdn.net *.fbsbx.com
https://fonts.gstatic.com;img-src *.fbcdn.net *.facebook.com data: https://*.fbsbx.com facebook.com
*.cdninstagram.com fbsbx.com fbcdn.net connect.facebook.net blob: android-webview-video-poster:
*.whatsapp.net *.fb.com *.oculuscdn.com *.tenor.co *.tenor.com *.giphy.com https://trustly.one/
https://*.trustly.one/ https://paywithmybank.com/ https://*.paywithmybank.com/
https://www.googleadservices.com https://googleads.g.doubleclick.net
https://*.google-analytics.com;media-src *.cdninstagram.com blob: *.fbcdn.net *.fbsbx.com
www.facebook.com *.facebook.com data: *.tenor.co *.tenor.com https://*.giphy.com;child-src data: blob:
'self' https://*.fbsbx.com *.facebook.com *.fbcdn.net;frame-src *.facebook.com *.fbsbx.com fbsbx.com
data: www.instagram.com *.fbcdn.net accounts.meta.com *.accounts.meta.com https://trustly.one/
https://*.trustly.one/ https://paywithmybank.com/ https://*.paywithmybank.com/
https://www.googleadservices.com https://googleads.g.doubleclick.net https://www.google.com
https://td.doubleclick.net *.google.com *.doubleclick.net;manifest-src data: blob: 'self'
https://*.fbsbx.com *.facebook.com *.fbcdn.net;object-src data: blob: 'self' https://*.fbsbx.com
*.facebook.com *.fbcdn.net;worker-src blob: *.facebook.com
data:;block-all-mixed-content;upgrade-insecure-requests;
```

X-Frame-Options Presente

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

Valor: DENY

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: accelerometer=(), attribution-reporting=(self), autoplay=(), bluetooth=(), browsing-topics=(self), camera=(self "https://www.fbsbx.com"), ch-device-memory=(), ch-downlink=(), ch-dpr=(), ch-ect=(), ch-rtt=(), ch-save-data=(), ch-ua-arch=(), ch-ua-bitness=(), ch-viewport-height=(), ch-viewport-width=(), ch-width=(), clipboard-read=(self), clipboard-write=(self), compute-pressure=(), display-capture=(self), encrypted-media=(self), fullscreen=(self), gamepad=*, geolocation=(self), gyroscope=(), hid=(), idle-detection=(), interest-cohort=(self), keyboard-map=(), local-fonts=(), magnetometer=(), microphone=(self), midi=(), otp-credentials=(), payment=(), picture-in-picture=(self), private-state-token-issuance=(), publickey-credentials-get=(self), screen-wake-lock=(), serial=(), shared-storage=(), shared-storage-select-url=(), private-state-token-redemption=(), usb=(), unload=(self), window-management=(), xr-spatial-tracking=(self);report-to="permissions_policy"

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