[CIBERPLANETA]

Security Headers Report

Análisis de cabeceras de seguridad HTTP

Objetivo:
`https://av-payment-static-dev.newshore.es/es/booking/payment/?pnr=BCND9R&tabId=5c89f4d1-f4b3-46ce-b42a-7d5c72`

Generado: 17/06/2026 13:03

80%

Seguridad

Riesgo Bajo

URL analizada:
`https://av-payment-static-dev.newshore.es/es/booking/payment/?pnr=BCND9R&tabId=5c`

9	6	3
Analizados	Presentes	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= 63072000; includeSubdomains; 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: frame-ancestors 'self' viajala.com.co *.viajala.com.co viajala.com.ec *.viajala.com.ec *.vuelosmuybaratos.com spinner.mauction.app *.kayak.com *.kayak.com.co *.kayak.co.uk *.kayak.es *.kayak.com.mx *.kayak.com.ar *.kayak.cl *.kayak.com.br *.cheapflights.com *.checkfelix.com *.mundi.com.br *.swoodoo.com *.momondo.com; upgrade-insecure-requests; default-src 'self' 'unsafe-inline' 'unsafe-eval' data: blob: *.avianca.com *.amadeus.com *.gstatic.com *.google-analytics.com *.googleapis.com *.googletagmanager.com *.googlesyndication.com *.google.com *.adobedtm.com *.go-mpulse.net *.akstat.io *.demdex.net *.qualtrics.com *.doubleclick.net *.fullstory.com fullstory.com *.everesttech.net *.online-metrix.net *.viajala.com viajala.com connect.facebook.net acutsdev.112.2o7.net eba-amadeus.netdna-ssl.com www.facebook.com bat.bing.com acutsprod.112.2o7.net www.google.com www.google.com.co www.googleadservices.com aeroviasdelcontinent.tt.omtrdc.net www.securitytrfx.com *.jquery.com *.angularjs.org *.aspnetcdn.com *.bootstrapcdn.com *.dwin1.com *.sleeknote.com *.mathtag.com *.liveperson.net *.sddan.com *.lpsnmedia.net *.acsbapp.com *.newshore.es *.entelgystats.com *.adnxs.com *.windows.net *.azure-api.net *.google adservice.google.com adservice.google.com.co *.telefonica.com *.avtest.ink *.googleusercontent.com *.fbcdn.net *.fbsbx.com *.youtube.com restcountries.eu *.restcountries.eu *.cloudfront.net cdnjs.cloudflare.com *.airtrfx.com *.jtdwjcwq6f4wp4ce.com *.everymundo.net *.sumologic.com *.everymundonet.work *.azurewebsites.net *.ipapi.co ipapi.co *.azureedge.net *.volantio.com unpkg.com *.criteo.com *.plusgrade.com fonts.cdnfonts.com *.akamaihd.net *.criteo.net *.onelinkbpo.com *.3dseatmapvr.com feedbucket.app *.feedbucket.app *.cookielaw.org *.modirum.com *.onetrust.com *.jsdelivr.net *.creativecdn.com *.cookiepro.com analytics.tiktok.com *.smartvel.com us1.zonkasurvey.com us-js.zonka.co *.global.ssl.fastly.net cm.adform.net ih.adscale.de visitor.omnitagjs.com pixel.advertising.com ice.360yield.com dsum-sec.casalemedia.com pixel.rubiconproject.com hbx.media.net cm.mgid.com onetag-sys.com us-u.openx.net sync.outbrain.com simage2.pubmatic.com bh.contextweb.com s.seedtag.com match.sharethrough.com s.ad.smaato.net us.ck-ie.com ce.lijit.com sync.taboola.com eb2.3lift.com s-cs.rmp.rakuten.com dot.wp.pl ad.yieldlab.net ads.yieldmo.com t.visx.net ssc-cms.33across.com pixel.s3xified.com inv-nets.admixer.net sync.e-planning.net csync.loopme.me adn.caprofitx.com sync.addlv.smt.docomo.ne.jp sync.teads.tv rt.udmserve.net sync.console.adtarget.com.tr sync.1rx.io ssp-csync.smartadserver.com rtb.gumgum.com sync.connectad.io csync.smilewanted.com a.vidoomy.com sync.cenarius.orangeclickmedia.com sync.go.sonobi.com fast.nexx360.io cm-exchange.toast.com ad.as.amanad.adtdp.com sync.bidence.net cs.gssprt.jp sp.gmossp-sp.jp analytics.ad.daum.net s-cs.send.microad.jp mixer.mobon.net tg.socdm.com sync.ad-stir.com *.mczbf.com *.skyscanner.net rum.browser-intake-datadoghq.com www.datadoghq-browser-agent.com *.riskified.com edge.adobedc.net *.zdassets.com *.zendesk.com *.centribal.com *.securitytrfx.com centinelapi.cardinalcommerce.com static.ads-twitter.com browser-intake-datadoghq.com api.datadoghq.com ims-na1.adobelogin.com dcs.adobedc.net cdn1.adoberesources.net centinelapistag.cardinalcommerce.com cas.client.cardinaltrusted.com;

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: 1; mode=block

Referrer-Policy PRESENTE

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

Valor: `same-origin`

Headers Faltantes (3)

Permissions-Policy (Feature-Policy) FALTANTE MEDIO

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

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

X-Permitted-Cross-Domain-Policies FALTANTE BAJO

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

Recomendación: none

COEP (Cross-Origin Embedder Policy) FALTANTE BAJO

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

Recomendación: require-corp