

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://bilbaoexhibitioncentre.com
Dominio bilbaoexhibitioncentre.com
Fecha 20 de julio de 2026 a las 06:54

Checks 9 pruebas
Hallazgos 45 totales
Problemas 7 detectados

B

86/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre bilbaoexhibitioncentre.com ha resultado en una puntuación de 86/100 con una nota de B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 5 finalizaron correctamente y 4 generaron advertencias de seguridad, sin detectarse fallos críticos totales. Los principales riesgos identificados se centran en la ausencia de cabeceras de transporte seguro y la exposición de puertos innecesarios. En su estado actual, el sitio se considera mayoritariamente seguro, aunque presenta debilidades configurativas que lo hacen vulnerable a técnicas de reconocimiento y ataques de intermediario.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 80 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 80 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
80 dias restantes (expira: 2026-10-08T02:12:08.000Z)
- INFO Fecha de emision
Emitido desde: 2026-07-10T01:12:24.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

- BAJO Server header expuesto
Server: cloudflare — Revela tecnologia del servidor

- INFO

Content-Security-Policy
Presente: default-src 'none'; script-src 'nonce-NISA8FOTsjZZTpbjUZNYvz' 'unsafe-eval' http...
- INFO

X-Frame-Options
Presente: SAMEORIGIN
- ALTO

Strict-Transport-Security
Falta — Fuerza conexiones HTTPS (HSTS)
- INFO

X-Content-Type-Options
Presente: nosniiff
- INFO

Referrer-Policy
Presente: same-origin
- INFO

Permissions-Policy
Presente: accelerometer=(),camera=(),clipboard-read=(),clipboard-write=(),geolocation=(),g...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://bilbaoexhibitioncentre.com/
- ALTO

HSTS (Strict-Transport-Security)
HSTS no configurado — El navegador no fuerza HTTPS
- INFO

Respuesta HTTPS
HTTPS responde con status 403

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO

WordPress
No detectado
- INFO

Joomla
No detectado
- INFO

Drupal
No detectado
- INFO

Magento
No detectado
- INFO

Shopify
No detectado
- INFO

PrestaShop
No detectado
- INFO

Wix
No detectado
- INFO

Squarespace
No detectado

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO

Archivo /readme.html
No accesible (correcto)
- INFO

Archivo /README.txt
No accesible (correcto)
- INFO

Version CMS
No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

INFO

Cookies detectadas
El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

INFO

Contenido mixto
Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

INFO

robots.txt
Presente (1715 bytes)

INFO

Reglas robots.txt
41 Disallow, 0 Allow

MEDIO

Bloqueo total
robots.txt bloquea todo el sitio con Disallow: /

BAJO

Ruta sensible en robots.txt
Referencia a "admin" — Puede revelar rutas sensibles a atacantes

BAJO

sitemap.xml
No encontrado (HTTP 403)

BAJO

security.txt
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

INFO

Puerto 21 (FTP)
Cerrado — Transferencia de archivos sin cifrar

INFO

Puerto 22 (SSH)
Cerrado — Acceso remoto seguro

INFO

Puerto 23 (Telnet)
Cerrado — Acceso remoto sin cifrar

INFO

Puerto 25 (SMTP)
Cerrado — Envio de correo

INFO

Puerto 80 (HTTP)
Abierto (esperado) — Servidor web

INFO

Puerto 443 (HTTPS)
Abierto (esperado) — Servidor web seguro

INFO

Puerto 3306 (MySQL)
Cerrado — Base de datos MySQL expuesta

INFO

Puerto 3389 (RDP)
Cerrado — Escritorio remoto Windows

INFO

Puerto 5432 (PostgreSQL)
Cerrado — Base de datos PostgreSQL expuesta

INFO

Puerto 6379 (Redis)
Cerrado — Cache Redis sin autenticacion por defecto

MEDIO

Puerto 8080 (HTTP-Alt)
ABIERTO — Servidor web alternativo / proxy

INFO

Puerto 27017 (MongoDB)
Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Strict-Transport-Security: La cabecera HSTS no está configurada, lo que impide que el servidor obligue al navegador a usar siempre conexiones cifradas.

[HIGH] HSTS (Strict-Transport-Security): Al no forzar HTTPS mediante esta política, el sitio es susceptible a ataques de degradación de SSL (SSL Stripping).

[MEDIUM] Puerto 8080 (HTTP-Alt): El puerto 8080 se encuentra abierto, lo que indica la presencia de un servidor alternativo o proxy que amplía innecesariamente la superficie de exposición.

[MEDIUM] Bloqueo total en robots.txt: El archivo robots.txt utiliza la instrucción Disallow: /, impidiendo el rastreo legítimo y sugiriendo una configuración de entorno de pruebas.

[LOW] Server header expuesto: La cabecera revela el uso de tecnología Cloudflare, lo que facilita a potenciales atacantes el reconocimiento de la infraestructura de red.

[LOW] Ruta sensible en robots.txt: La mención de la palabra admin dentro del archivo de rastreo proporciona pistas directas sobre la ubicación de paneles de gestión internos.

[LOW] sitemap.xml: El archivo de mapa del sitio no fue localizado debido a una respuesta de error 403, lo que dificulta la verificación de la estructura web.