

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://eldagrandeotravez.es/
Dominio eldagrandeotravez.es
Fecha 6 de octubre de 2026 a las 09:57

Checks 9 pruebas
Hallazgos 42 totales
Problemas 11 detectados

C

68/100

puntos de seguridad



RESUMEN EJECUTIVO

Tras realizar la auditoría técnica, el sitio web ha obtenido una puntuación de seguridad de 68/100, lo que se traduce en una calificación de nota C. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron identificados como fallos críticos. Aunque el cifrado SSL básico es correcto, la ausencia total de cabeceras de seguridad y la exposición de servicios de transferencia de archivos inseguros comprometen la integridad de la plataforma. En su estado actual, el sitio se considera vulnerable a ataques de interceptación de datos y manipulación de contenido.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 31 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 31 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
31 dias restantes (expira: 2026-11-05T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-04-21T00:00:00.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- ALTO

Content-Security-Policy
Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO

X-Frame-Options
Falta — Protege contra clickjacking
- ALTO

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

X-Content-Type-Options
Falta — Evita MIME-type sniffing
- MEDIO

Referrer-Policy
Falta — Controla la informacion de referer enviada
- MEDIO

Permissions-Policy
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://eldagrandeotravez.es/
- ALTO

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

Respuesta HTTPS
HTTPS responde con status 200

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 — 20/100

Estado: FALLO
Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
No encontrado (HTTP 404)
- BAJO **sitemap.xml**
No encontrado (HTTP 404)
- BAJO **security.txt**
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO
1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- ALTO **Puerto 21 (FTP)**
ABIERTO — 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
- INFO **Puerto 8080 (HTTP-Alt)**
Cerrado — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Puerto 21 (FTP): El puerto de transferencia de archivos está abierto y permite el envío de datos y credenciales sin cifrado, lo que facilita el robo de información.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido como Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking, donde un atacante puede engañar al usuario para que realice acciones no deseadas.
[HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, permitiendo que un atacante pueda degradar la conexión a una versión HTTP no segura.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite al navegador adivinar el tipo de contenido, lo que puede ser explotado para ejecutar archivos maliciosos disfrazados.

[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia que se envía a otros dominios, lo que podría filtrar rutas internas o datos sensibles.

[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador para acceder a hardware o APIs, dejando expuesta la privacidad del usuario ante posibles scripts.

[LOW] Server header expuesto: La cabecera revela el uso de nginx, proporcionando información técnica valiosa que un atacante puede usar para buscar exploits específicos.

[LOW] Archivos de rastreo faltantes: La ausencia de robots.txt y sitemap.xml dificulta la gestión adecuada del sitio por parte de los motores de búsqueda y la auditoría de rutas.