EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://carranzais.es/en/	Checks	9 pruebas
Dominio	carranzais.es	Hallazgos	40 totales
Fecha	8 de mayo de 2026 a las 17:18	Problemas	11 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio web carranzais.es arroja una puntuacion de 68/100, lo que equivale a una nota C. Los resultados se derivan de la ejecucion de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 presentaron advertencias y 2 fallaron de forma critica. Aunque el cifrado de datos es correcto, la ausencia total de cabeceras de seguridad y la exposicion de servicios administrativos incrementan el riesgo de ataques dirigidos. En su estado actual, el sitio se considera vulnerable debido a configuraciones deficientes que comprometen la proteccion contra inyecciones y el secuestro de sesiones.

Resumen de Riesgos

0	4	6	1	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 89 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): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 89 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  89 dias restantes (expira: 2026-08-05T16:27:02.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-07T16:27:03.000Z
- 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/1.22.1 — 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://carranzais.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

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- 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

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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] Content-Security-Policy: Falta esta cabecera, lo que permite la ejecucion de ataques de inyeccion de scripts (XSS) y contenido malicioso.
[HIGH] X-Frame-Options: No detectada, dejando el sitio expuesto a ataques de clickjacking donde un atacante puede camuflar la interfaz.
[HIGH] Strict-Transport-Security: La ausencia de HSTS impide que el navegador fuerce siempre conexiones seguras, permitiendo posibles degradaciones de protocolo.
[MEDIUM] X-Content-Type-Options: Falta esta directiva, permitiendo que el navegador adivine el tipo de contenido y ejecute archivos peligrosos.
[MEDIUM] Referrer-Policy: No configurada, lo que puede provocar la fuga de informacion sensible en las URL hacia sitios externos.
[MEDIUM] Permissions-Policy: Falta esta cabecera, dejando sin control el acceso del navegador a funciones como la camara, microfono o geolocalizacion.
[MEDIUM] Archivo /readme.html y /README.txt: Estos archivos son accesibles publicamente y pueden revelar informacion tecnica sobre la estructura del sitio.
[MEDIUM] Puerto 22 (SSH): El puerto de acceso remoto se encuentra abierto, lo que representa un punto de entrada para intentos de intrusion por fuerza bruta.
[LOW] Server header expuesto: El servidor revela el uso de nginx/1.22.1, informacion que ayuda a atacantes a buscar vulnerabilidades especificas de esa version.
[LOW] Robots.txt y Sitemap: La falta de estos archivos indica una gestion deficiente del rastreo y puede exponer rutas que no deberian ser publicas.