EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://zarandeo.es/	Checks	9 pruebas
Dominio	zarandeo.es	Hallazgos	43 totales
Fecha	15 de mayo de 2026 a las 12:28	Problemas	8 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 76/100, lo que equivale a una nota B. Se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 generó una advertencia y 2 finalizaron con errores críticos. El cifrado de datos es correcto, pero existen fallos graves en la configuración del servidor y en la protección contra ataques de inyección. Debido a la exposición de servicios críticos y la falta de cabeceras de seguridad, se concluye que el sitio es actualmente vulnerable a ataques dirigidos.

Resumen de Riesgos

1	5	1	1	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 83 dias
Cabeceras de Seguridad	40	FALLO	Solo 3/6 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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 83 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  83 dias restantes (expira: 2026-08-06T11:25:08.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-08T11:25:09.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 40/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security

- BAJO **Server header expuesto**
  Server: HTTPd — 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)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: interest-cohort=()

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://zarandeo.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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (687 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 13 Allow
- INFO **Sitemap en robots.txt**
  https://zarandeo.es/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL): Abierto. La base de datos es accesible desde internet, lo que permite intentos de acceso no autorizado y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP): Abierto. Este protocolo transmite datos y credenciales sin cifrar, facilitando la interceptación de información sensible.
[HIGH] Content-Security-Policy (CSP): Falta. La ausencia de esta política permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).
[HIGH] X-Frame-Options: Falta. El sitio es vulnerable a ataques de Clickjacking, donde un atacante puede engañar al usuario para que realice acciones no deseadas.

[HIGH] Strict-Transport-Security (HSTS): Falta. El servidor no obliga al navegador a usar siempre conexiones seguras, permitiendo ataques de degradación de protocolo.
[MEDIUM] Puerto 22 (SSH): Abierto. Aunque es un acceso seguro, mantenerlo expuesto públicamente aumenta la superficie de ataque para accesos remotos al servidor.
[LOW] Cabecera Server expuesta: Server: HTTPd. Revelar la tecnología exacta del servidor facilita a los atacantes la búsqueda de vulnerabilidades específicas para esa versión.