

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://emrodriguez.es
Dominio emrodriguez.es
Fecha 23 de marzo de 2026 a las 21:51

Checks 9 pruebas
Hallazgos 45 totales
Problemas 7 detectados

B

83/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el dominio emrodriguez.es ha dado como resultado una puntuación de 83/100, lo que corresponde a una nota B. Durante la evaluación se ejecutaron 9 checks pasivos, identificando 6 puntos configurados correctamente y 3 advertencias de seguridad que requieren atención inmediata. A pesar de contar con un cifrado SSL óptimo, la ausencia de cabeceras de seguridad críticas y la apertura de puertos no estándar elevan el nivel de riesgo. Se concluye que el sitio web es mayoritariamente seguro, pero presenta vulnerabilidades de configuración que podrían ser explotadas para realizar ataques de inyección o interceptación.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 61 dias
Cabeceras de Seguridad	55	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 61 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
61 dias restantes (expira: 2026-05-23T21:25:09.000Z)
- INFO Fecha de emision
Emitido desde: 2026-02-22T20:26:44.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security

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

- ALTO

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

X-Frame-Options
Presente: SAMEORIGIN
- ALTO

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

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

Referrer-Policy
Presente: same-origin
- INFO

Permissions-Policy
Presente: accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-write=...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://emrodriguez.es/
- 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO

robots.txt
Presente (1853 bytes)
- INFO

Reglas robots.txt
10 Disallow, 2 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
- INFO

Sitemap en robots.txt
<https://emrodriguez.es/wp-sitemap.xml>
- 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] Content-Security-Policy (CSP) ausente: La falta de esta cabecera permite ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso en el navegador del usuario.

[HIGH] Strict-Transport-Security (HSTS) faltante: El servidor no obliga al navegador a usar conexiones cifradas, lo que permite ataques de degradación de HTTPS a HTTP.

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este puerto alternativo puede revelar servicios de administración o proxies que no deberían ser accesibles públicamente.

[MEDIUM] Robots.txt con bloqueo total: El archivo bloquea el rastreo de todo el sitio, lo cual es inusual y puede esconder configuraciones o rutas que no deberían estar expuestas.

[LOW] Server header expuesto: El servidor revela el uso de la tecnología Cloudflare, facilitando a un atacante potencial la identificación de la infraestructura de red.

[LOW] Ruta sensible en robots.txt: Se menciona la ruta admin en el archivo de rastreo, lo cual ofrece pistas directas sobre la ubicación de posibles paneles de gestión.

[INFO] Respuesta HTTPS 403: Al intentar acceder vía HTTPS, el servidor devuelve un código de estado de acceso prohibido, sugiriendo una restricción de permisos o configuración incompleta.