

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://marianojb.es/	Checks	9 pruebas
Dominio	marianojb.es	Hallazgos	43 totales
Fecha	6 de octubre de 2026 a las 10:01	Problemas	11 detectados

C

68/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el sitio web arroja una puntuación de 68/100, lo que otorga una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron clasificados como fallos. Aunque el sitio cuenta con un cifrado SSL robusto, la ausencia total de cabeceras de seguridad y la exposición de servicios críticos representan un riesgo considerable. Se concluye que el sitio es actualmente vulnerable a ataques de inyección y suplantación, por lo que requiere intervenciones técnicas inmediatas.

Resumen de Riesgos

0 CRITICO	5 ALTO	3 MEDIO	3 BAJO	32 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 192 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 192 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
192 dias restantes (expira: 2027-04-15T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-29T00:00:00.000Z
- 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://marianojb.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
- INFO

Tecnologias detectadas
Next.js

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) ABIERTO: Permite la transferencia de archivos sin cifrar, lo que facilita la interceptación de credenciales y datos por terceros.

[HIGH] Content-Security-Policy Faltante: La ausencia de esta cabecera impide prevenir ataques de Cross-Site Scripting (XSS) e inyecciones de contenido malicioso.

[HIGH] X-Frame-Options Faltante: El sitio es vulnerable a ataques de clickjacking al permitir que el contenido sea cargado en frames de sitios externos.

[HIGH] Strict-Transport-Security (HSTS) Faltante: No se obliga al navegador a utilizar exclusivamente conexiones HTTPS, permitiendo posibles degradaciones de seguridad.

[MEDIUM] X-Content-Type-Options Faltante: El navegador podría realizar MIME-type sniffing, ejecutando archivos con tipos de contenido incorrectos o peligrosos.

[MEDIUM] Referrer-Policy Faltante: No existe control sobre la información de navegación que se comparte con otros dominios al hacer clic en enlaces.

[MEDIUM] Permissions-Policy Faltante: No se restringen las capacidades de las APIs del navegador, como el acceso a la cámara o el micrófono.

[LOW] Server Header Expuesto: La cabecera revela que el servidor utiliza nginx, proporcionando información útil para que un atacante busque exploits específicos.

[LOW] Archivos robots.txt y sitemap.xml Faltantes: La falta de estos archivos dificulta el control del rastreo y la indexación correcta de la estructura web.