

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ebcol360.com/	Checks	9 pruebas
Dominio	ebcol360.com	Hallazgos	44 totales
Fecha	17 de septiembre de 2026 a las 01:28	Problemas	5 detectados

B

84/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio ebcol360.com arrojó una puntuación de 84/100, lo que equivale a una nota B. Se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 fue calificado como fallo. El dominio demuestra una implementación sólida de cifrado SSL y políticas de redirección segura, aunque presenta carencias en cabeceras de seguridad y gestión de archivos de rastreo. En conclusión, el sitio se considera generalmente seguro, pero vulnerable a ataques específicos de inyección y exposición de servicios administrativos debido a configuraciones pendientes.

Resumen de Riesgos

0 CRITICO	1 ALTO	2 MEDIO	2 BAJO	39 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 88 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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 88 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
88 dias restantes (expira: 2026-12-13T23:26:22.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-14T23:26:23.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

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

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

- INFO

X-Frame-Options
Presente: DENY
- INFO

Strict-Transport-Security
Presente: max-age=31536000
- INFO

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

Referrer-Policy
Presente: same-origin
- MEDIO

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

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

HTTP !' HTTPS redireccion
HTTP 308 redirige a https://ebcol360.com/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=31536000
- BAJO

HSTS includeSubDomains
HSTS no cubre subdominios
- INFO

HSTS max-age
max-age=31536000 (365 días)
- 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
React, 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): 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: La ausencia de esta cabecera permite la ejecución de scripts no autorizados, facilitando ataques de Cross-Site Scripting (XSS) e inyección de datos.
[MEDIUM] Permissions-Policy: La falta de esta configuración impide restringir el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.

[MEDIUM] Puerto 22 (SSH) abierto: La exposición pública de este puerto de administración remota aumenta el riesgo de ataques de fuerza bruta dirigidos a obtener acceso al servidor.

[LOW] robots.txt no encontrado: La carencia de este archivo deja al sitio sin instrucciones para los motores de búsqueda sobre qué directorios deben evitarse.

[LOW] sitemap.xml no encontrado: La falta de este documento dificulta la indexación estructurada y puede exponer rutas que no deberían ser públicas de forma involuntaria.