EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://compositor.org/	Checks	9 pruebas
Dominio	compositor.org	Hallazgos	46 totales
Fecha	10 de mayo de 2026 a las 18:51	Problemas	13 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha resultado en una puntuación de 59/100, lo que equivale a una nota de D. Se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron calificados como fallos críticos. Aunque el cifrado de transporte es correcto, la ausencia total de cabeceras de seguridad y la exposición de servicios obsoletos elevan el riesgo técnico. En su estado actual, el sitio se considera vulnerable debido a configuraciones de servidor deficientes que comprometen la integridad de la conexión.

Resumen de Riesgos

0	6	4	3	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 37 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 37 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  37 dias restantes (expira: 2026-06-17T02:45:03.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-19T02:45:04.000Z
- 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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.1.29, PleskLin — Revela framework/lenguaje
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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**
  PHP/8.1.29, PleskLin

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (26 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- 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] Falta de redireccion HTTP a HTTPS: El sitio permite conexiones a través de HTTP sin redirigir al protocolo seguro, exponiendo los datos a interceptación.
[HIGH] HSTS (Strict-Transport-Security) no configurado: La ausencia de esta política impide que los navegadores fuercen siempre una conexión cifrada, facilitando ataques de degradación de SSL.
[HIGH] Content-Security-Policy (CSP) ausente: La falta de esta cabecera permite ataques de inyección de contenido y Cross-Site Scripting (XSS) al no restringir las fuentes de scripts.
[HIGH] X-Frame-Options ausente: El sitio es vulnerable a ataques de clickjacking, ya que permite ser cargado dentro de frames o iframes externos.
[HIGH] Puerto 21 (FTP) abierto: Este servicio de transferencia de archivos transmite credenciales y datos en texto plano, siendo un vector crítico de compromiso de cuentas.
[MEDIUM] X-Content-Type-Options ausente: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido (MIME-sniffing), lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy ausente: No existe control sobre la información de navegación que se envía a sitios externos cuando un usuario hace clic en un enlace.
[MEDIUM] Permissions-Policy ausente: No se restringe el acceso del navegador a funciones sensibles como la cámara, el micrófono o la ubicación desde el contexto web.
[MEDIUM] Bloqueo total en robots.txt: La directiva Disallow: / bloquea toda indexación legítima, lo cual suele ser síntoma de una configuración de desarrollo olvidada en producción.
[LOW] Server header expuesto: El encabezado revela que el servidor utiliza nginx, proporcionando información útil para que un atacante busque exploits específicos.
[LOW] X-Powered-By expuesto: Se revela el uso de PHP/8.1.29 y PleskLin, lo cual facilita el reconocimiento de la infraestructura y sus posibles debilidades.
[LOW] sitemap.xml no encontrado: La falta de este archivo dificulta la auditoría de contenidos y la navegación estructurada para herramientas de seguridad.