EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cosantafesino.com.ar	Checks	9 pruebas
Dominio	cosantafesino.com.ar	Hallazgos	46 totales
Fecha	7 de abril de 2026 a las 18:06	Problemas	16 detectados

F

39/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio cosantafesino.com.ar arroja un resultado critico con una puntuacion de 39/100 y una nota de F. Los checks pasivos ejecutados identificaron fallos significativos, con solo 3 pruebas superadas frente a 5 fallos graves y una advertencia. Se detectaron deficiencias estructurales en la configuracion del servidor y el uso de software extremadamente obsoleto. Por lo tanto, el sitio se clasifica como vulnerable y no cumple con los estandares minimos de ciberseguridad actuales.

Resumen de Riesgos

0	8	5	3	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 88 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	20	FALLO	WordPress 2.0 expuesta
Seguridad de Cookies	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

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: 2026-07-05T03:34:24.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-06T03:34:25.000Z
- 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: Apache — 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 — 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**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 2.0 expuesta

- ALTO **WordPress version**
  Version 2.0 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)

Seguridad de Cookies — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.cosantafesino.com.ar/turnos

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 — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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] WordPress version: Version 2.0 expuesta publicamente. Es una version extremadamente antigua que permite a atacantes explotar multiples CVEs conocidos y tomar el control del sitio.

[HIGH] Content-Security-Policy: Falta esta cabecera. Su ausencia facilita ataques de Cross-Site Scripting (XSS) y la inyeccion de contenido malicioso.
[HIGH] X-Frame-Options: Falta esta cabecera. Deja el sitio desprotegido ante ataques de clickjacking, donde un atacante puede engañar al usuario para que realice acciones no deseadas.
[HIGH] Strict-Transport-Security: Falta configuracion HSTS. El navegador no fuerza conexiones cifradas, permitiendo posibles ataques de degradacion de SSL.
[HIGH] Redireccion HTTPS: No hay redireccion de HTTP a HTTPS. Las comunicaciones pueden ser interceptadas ya que el servidor permite el acceso mediante el protocolo no seguro.
[HIGH] Cookie PHPSESSID: Faltan flags HttpOnly y Secure. La cookie de sesion es accesible mediante scripts del navegador y se envia a traves de conexiones no cifradas.
[MEDIUM] X-Content-Type-Options: Falta esta cabecera. Permite el sniffing de tipos MIME, lo que puede llevar a la ejecucion de archivos maliciosos disfrazados de elementos legitimos.
[MEDIUM] Cookie PHPSESSID: Falta flag SameSite. El sitio es vulnerable a ataques de falsificacion de peticion en sitios cruzados (CSRF).
[MEDIUM] Referrer-Policy: Falta esta cabecera. No se controla la cantidad de informacion que el navegador envia al saltar a otros enlaces.
[MEDIUM] Permissions-Policy: Falta esta cabecera. No se restringe el acceso de las APIs del navegador a funciones sensibles como camara o microfono.
[MEDIUM] Contenido Mixto: Se detecto un recurso HTTP (enlace de turnos) cargando dentro de la pagina HTTPS, lo que rompe la integridad del cifrado.
[LOW] Server header expuesto: Se muestra la tecnologia Apache. Esta informacion ayuda a los atacantes a buscar vulnerabilidades especificas del software del servidor.
[LOW] Archivos de indexacion: Faltan robots.txt y sitemap.xml. Dificulta la gestion del rastreo por parte de motores de busqueda y la visibilidad de la estructura del sitio.