EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.macronegocios.ec	Checks	9 pruebas
Dominio	www.macronegocios.ec	Hallazgos	48 totales
Fecha	30 de marzo de 2026 a las 15:44	Problemas	12 detectados

C

74/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 74/100, lo que resulta en una calificación de grado C. Durante la evaluación se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 5 resultaron satisfactorias, 1 generó una advertencia y 3 fallaron debido a configuraciones incorrectas. Aunque el cifrado de datos es robusto, la ausencia de políticas de seguridad en el transporte y la gestión deficiente de las cookies de sesión incrementan el riesgo de ataques de intermediario. Por lo tanto, se concluye que el sitio es vulnerable ante vectores de ataque conocidos que podrían comprometer la sesión de los usuarios.

Resumen de Riesgos

0	5	4	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 57 dias
Cabeceras de Seguridad	55	FALLO	Solo 3/6 presentes. Faltan: Strict-Transport-Sec...
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	17	FALLO	frontend_lang: falta HttpOnly; frontend_lang: fa...
Contenido Mixto	100	OK	No se detecto contenido mixto
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 57 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  57 dias restantes (expira: 2026-05-26T22:07:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-25T22:08:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx/1.18.0 (Ubuntu) — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: frame-ancestors 'self'
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN, SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff, nosniff
- 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://www.macronegocios.ec/
- 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

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 — 17/100

Estado: FALLO

frontend_lang: falta HttpOnly; frontend_lang: falta Secure; frontend_lang: falta SameSite; session_id: falta Secure; session_id: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: frontend_lang — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: frontend_lang — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: frontend_lang — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: session_id — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: session_id — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: session_id — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 — 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] Strict-Transport-Security: La ausencia de la cabecera HSTS impide que el navegador fuerce conexiones cifradas, permitiendo ataques de degradación de protocolo.
[HIGH] Cookie frontend_lang (HttpOnly): La falta de este flag permite que la cookie sea accesible mediante scripts del lado del cliente, facilitando ataques de XSS.
[HIGH] Cookie frontend_lang (Secure): Al no tener el flag Secure, esta cookie puede ser transmitida a través de conexiones HTTP no cifradas.
[HIGH] Cookie session_id (Secure): La falta de este flag permite que el identificador de sesión viaje por canales inseguros, facilitando el secuestro de la cuenta.
[MEDIUM] Cookie frontend_lang (SameSite): La omisión de este atributo deja al usuario desprotegido ante posibles ataques de falsificación de solicitud en sitios cruzados (CSRF).
[MEDIUM] Cookie session_id (SameSite): La ausencia de protección SameSite en la sesión principal incrementa el riesgo de acciones no autorizadas mediante CSRF.
[MEDIUM] Referrer-Policy: No existe una política definida, lo que puede provocar la fuga de información sensible en las cabeceras de navegación hacia sitios externos.
[MEDIUM] Permissions-Policy: La falta de esta cabecera impide restringir el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[LOW] Server header expuesto: El servidor revela la versión exacta de la tecnología utilizada (nginx/1.18.0 Ubuntu), facilitando la búsqueda de exploits específicos.
[LOW] Archivos robots.txt y sitemap.xml: La inexistencia de estos archivos dificulta la correcta indexación y el reconocimiento de la estructura del sitio por agentes legítimos.