EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://macrisal.com	Checks	9 pruebas
Dominio	macrisal.com	Hallazgos	47 totales
Fecha	12 de mayo de 2026 a las 15:48	Problemas	14 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del dominio macrisal.com ha dado como resultado una puntuación de 64/100, lo que corresponde a una calificación de grado C. Durante la auditoría se ejecutaron 9 checks pasivos, logrando 5 resultados satisfactorios, 2 advertencias y 2 fallos críticos relacionados con la configuración del servidor y el mantenimiento del software. No se realizó un pentest activo, por lo que los hallazgos se limitan a la superficie de exposición pública. Se concluye que el sitio es actualmente vulnerable debido a la falta de cabeceras de seguridad esenciales y al uso de una versión de WordPress desactualizada.

Resumen de Riesgos

0	6	4	4	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 139 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	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 6.9.4 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 139 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  139 dias restantes (expira: 2026-09-28T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-01T00:00:00.000Z
- 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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.31, 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.macrisal.com/
- 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

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WPSSO Core 21.12.0/S
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.3.31, PleskLin

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta

- ALTO **WordPress version**
  Version 6.9.4 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 — 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (1007 bytes)
- INFO **Reglas robots.txt**
  16 Disallow, 0 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.macrisal.com/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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] WordPress version 6.9.4 expuesta: La versión del CMS es visible públicamente, lo que facilita a atacantes la búsqueda y explotación de vulnerabilidades CVE conocidas para esta compilación específica.
[HIGH] Falta de Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados, aumentando el riesgo de ataques de inyección de contenido y XSS.
[HIGH] Falta de X-Frame-Options: El sitio no bloquea su carga dentro de frames de terceros, lo que lo hace vulnerable a ataques de secuestro de clics o clickjacking.
[HIGH] Falta de Strict-Transport-Security: No se fuerza el uso de conexiones seguras mediante HSTS, permitiendo posibles ataques de degradación de protocolo SSL/TLS.
[HIGH] Puerto 21 (FTP) abierto: La presencia de este puerto expone un servicio de transferencia de archivos que no utiliza cifrado de forma nativa, permitiendo la interceptación de credenciales.
[MEDIUM] Falta de X-Content-Type-Options: La ausencia de esta cabecera permite que los navegadores intenten adivinar el tipo de contenido, facilitando ataques de tipo MIME-sniffing.
[MEDIUM] Falta de Referrer-Policy: No se controla la cantidad de información que el navegador envía al navegar desde este sitio hacia otros enlaces externos.
[MEDIUM] Falta de Permissions-Policy: El sitio no restringe el acceso a funciones sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Puerto 22 (SSH) abierto: El servicio de acceso remoto está expuesto, lo que aumenta la superficie de ataque para intentos de intrusión por fuerza bruta.
[LOW] Server header expuesto: El servidor revela el uso de nginx, proporcionando información técnica valiosa para la fase de reconocimiento de un atacante.
[LOW] X-Powered-By expuesto: Se detalla el uso de PHP/8.3.31 y PleskLin, permitiendo a los atacantes acotar sus vectores de ataque según el framework y entorno detectado.
[LOW] Meta generator expuesto: El código fuente revela el uso del plugin WPSSO Core 21.12.0/S.
[LOW] Ruta sensible en robots.txt: Se ha detectado una referencia directa al directorio admin, lo que ayuda a identificar rutas administrativas.