

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://macrofitinvest.com/
Dominio macrofitinvest.com
Fecha 18 de mayo de 2026 a las 03:50

Checks 9 pruebas
Hallazgos 50 totales
Problemas 7 detectados

C

70/100

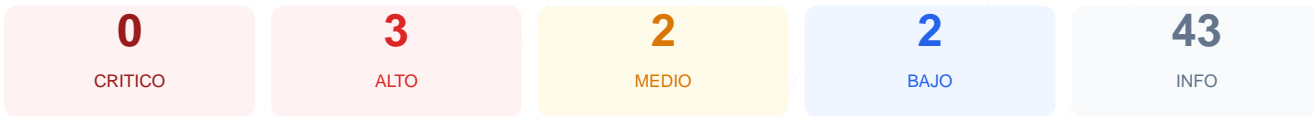
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad del sitio macrofitinvest.com ha resultado en una puntuación de 70/100, lo que equivale a una nota de C. Se ejecutaron un total de 9 controles pasivos, de los cuales 6 resultaron satisfactorios, uno presentó advertencias y dos fallaron de forma crítica. El sitio presenta deficiencias importantes en la implementación de políticas de seguridad modernas y en la redirección obligatoria de tráfico cifrado. Debido a la ausencia de cabeceras de protección esenciales y la exposición de puertos alternativos, el sitio se considera vulnerable a ataques de intermediario y secuestro de clics. Se requiere una intervención técnica para mejorar la postura defensiva de la plataforma antes de que sea explotada.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 83 dias
Cabeceras de Seguridad	45	FALLO	Solo 3/6 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	1 cookies, todas con flags correctos
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	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 83 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
83 dias restantes (expira: 2026-08-08T17:41:08.000Z)
- INFO Fecha de emision
Emitido desde: 2026-05-10T16:41:16.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 45/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Permissions-Policy

- BAJO Server header expuesto
Server: cloudflare — Revela tecnologia del servidor

- **ALTO** **Content-Security-Policy**
Falta — Previene XSS y ataques de inyección de contenido
- **ALTO** **X-Frame-Options**
Falta — Protege contra clickjacking
- **INFO** **Strict-Transport-Security**
Presente: max-age=31536000; includeSubDomains
- **INFO** **X-Content-Type-Options**
Presente: nosniiff
- **INFO** **Referrer-Policy**
Presente: strict-origin-when-cross-origin
- **MEDIO** **Permissions-Policy**
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redirección HTTPS — 0/100

Estado: **FALLO**

No hay redirección HTTP a HTTPS

- **ALTO** **HTTP !' HTTPS redirección**
HTTP 302 — No redirige a HTTPS
- **INFO** **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31536000; includeSubDomains
- **BAJO** **HSTS includeSubDomains**
HSTS cubre subdominios
- **INFO** **HSTS max-age**
max-age=31536000 (365 días)
- **INFO** **Respuesta HTTPS**
HTTPS responde con status 200

Detección CMS — 100/100

Estado: **OK**

No se detectó 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** **Tecnologías detectadas**
React

Version CMS Expuesta — 100/100

Estado: **OK**

No se detectó versión 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

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
1 cookie(s) encontrada(s)
- INFO **Cookie: __cf_bm — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __cf_bm — SameSite**
SameSite=none

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 (251 bytes)
- INFO **Reglas robots.txt**
2 Disallow, 5 Allow
- BAJO **Ruta sensible en robots.txt**
Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
<https://www.macrofitinvest.com/sitemap.xml>
- BAJO **security.txt**
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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)**
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
- **MEDIO** **Puerto 8080 (HTTP-Alt)**
ABIERTO — 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 maliciosos y ataques de inyección de contenido XSS.
- [HIGH] X-Frame-Options: La falta de esta protección facilita ataques de clickjacking, permitiendo que el sitio sea cargado en marcos externos no autorizados.
- [HIGH] Redirección HTTP a HTTPS: El sistema no fuerza el tráfico cifrado de forma automática mediante un código 301, exponiendo los datos de los usuarios.
- [MEDIUM] Puerto 8080 (HTTP-Alt): Este puerto se encuentra abierto, lo que aumenta la superficie de ataque al exponer un servidor web o proxy alternativo.
- [MEDIUM] Permissions-Policy: No se restringe el acceso a las APIs del navegador, como la cámara o el micrófono, aumentando los riesgos de privacidad del usuario.
- [LOW] Server header expuesto: Se revela el uso de tecnología Cloudflare, proporcionando información técnica útil para que un atacante planifique un vector de entrada.
- [LOW] Ruta sensible en robots.txt: El archivo menciona una ruta hacia un directorio de administración, lo cual facilita el reconocimiento de puntos críticos a atacantes.