# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://static-content.micro1.ai/ | Checks | 9 pruebas |
| Dominio | static-content.micro1.ai | Hallazgos | 42 totales |
| Fecha | 4 de mayo de 2026 a las 16:07 | Problemas | 11 detectados |

C

61/100

puntos de seguridad

## RESUMEN EJECUTIVO

El analisis de ciberseguridad realizado al sitio web ha arrojado una puntuacion de 61/100, lo que equivale a una nota de C. Se ejecutaron un total de 9 checks pasivos, resultando en 6 verificaciones exitosas y 3 fallos criticos detectados en la configuracion del servidor. A pesar de contar con un certificado SSL robusto, la ausencia total de cabeceras de seguridad y la falta de redireccion automatica a HTTPS comprometen la integridad del sitio. En su estado actual, el sitio se considera vulnerable a ataques de intermediario e inyeccion de contenido.

## Resumen de Riesgos

| 0 | 5 | 3 | 3 | 31 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 193 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 | 20 | FALLO | Faltan robots.txt y sitemap.xml |
| Puertos Abiertos | 100 | OK | 2 puerto(s) abierto(s), todos esperados |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 193 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  193 dias restantes (expira: 2026-11-13T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-10-15T00:00:00.000Z
- 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: AmazonS3 — 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 403 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

## 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 — 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

## Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecucion de scripts maliciosos y ataques de inyeccion de datos (XSS).
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking donde un tercero puede secuestrar clics del usuario.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones cifradas, facilitando ataques de degradacion de protocolo.
[HIGH] Redireccion HTTPS: El servidor responde con error 403 en lugar de redirigir el trafico de HTTP a HTTPS, dejando conexiones iniciales desprotegidas.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite el MIME-type sniffing, lo que podria derivar en la ejecucion de archivos con contenido inesperado.
[MEDIUM] Referrer-Policy: No se controla que informacion de procedencia se envia a otros sitios, lo que puede filtrar URLs privadas o parametros sensibles.

[MEDIUM] Permissions-Policy: No existen restricciones sobre el uso de hardware o APIs del navegador como camaras o geolocalizacion por parte de scripts externos.
[LOW] Server header expuesto: La cabecera Server revela explicitamente el uso de AmazonS3, proporcionando informacion valiosa para el reconocimiento por parte de atacantes.
[LOW] Archivos de indexacion faltantes: No se encontraron robots.txt ni sitemap.xml, lo que genera respuestas de error 403 y dificulta la gestion de rastreo.