EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://maxvinil.ceos.digital	Checks	9 pruebas
Dominio	maxvinil.ceos.digital	Hallazgos	43 totales
Fecha	12 de mayo de 2026 a las 13:49	Problemas	4 detectados

A

96/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el sitio web ha resultado en una puntuación de 96/100, lo que equivale a una calificación de nota A. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 7 resultaron conformes y 1 se identificó como advertencia, sin registrarse fallos críticos en la configuración analizada. Los resultados indican que la plataforma mantiene un estándar de seguridad elevado, con una implementación de cifrado excelente y una gestión adecuada de activos visibles. Se concluye que el sitio es seguro para su operación habitual, aunque requiere ajustes menores de endurecimiento para mitigar riesgos de divulgación de información y ataques de interfaz.

Resumen de Riesgos

0	1	1	2	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 79 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: X-Frame-Options
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 79 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  79 dias restantes (expira: 2026-07-31T01:01:40.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-02T01:01:41.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: X-Frame-Options

- BAJO **Server header expuesto**
  Server: Microsoft-IIS/10.0 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsa...
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(), microphone=(), camera=(), payment=()

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**
  Astro, ASP.NET

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (193 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://www.seusite.com/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

1 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)**
  Cerrado — 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] X-Frame-Options: Esta cabecera de seguridad no está presente, lo que permite que el sitio sea cargado dentro de iframes en dominios externos, facilitando ataques de Clickjacking.
[MEDIUM] Bloqueo total en robots.txt: El archivo utiliza la directiva Disallow: /, lo que impide que los motores de búsqueda indexen el contenido, afectando la visibilidad legítima del sitio.
[LOW] Server header expuesto: La cabecera revela la versión exacta del servidor Microsoft-IIS/10.0, proporcionando datos valiosos para que un atacante busque vulnerabilidades específicas del software.
[LOW] X-Powered-By expuesto: El servidor indica explícitamente el uso de ASP.NET, revelando el framework de desarrollo y reduciendo el esfuerzo de reconocimiento para posibles explotaciones dirigidas.