EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://club.matahevo.com	Checks	9 pruebas
Dominio	club.matahevo.com	Hallazgos	45 totales
Fecha	23 de abril de 2026 a las 10:39	Problemas	14 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha resultado en una puntuación de 59/100, lo que equivale a una calificación de grado D. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 5 resultaron satisfactorias, 2 generaron advertencias y 2 fueron marcadas como fallos críticos de configuración. Aunque el cifrado de datos básico está presente, la ausencia de políticas de seguridad en las cabeceras del servidor eleva significativamente el riesgo. Debido a estas deficiencias técnicas, se concluye que el sitio es vulnerable ante ataques de suplantación y manipulación de contenido.

Resumen de Riesgos

0	5	7	2	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 63 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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 63 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  63 dias restantes (expira: 2026-06-24T23:13:40.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-26T23:13:41.000Z
- 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: cloudflare — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Next.js — 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 307 — No redirige a HTTPS
- 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
- INFO **Tecnologias detectadas**
  React, Next.js, Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1738 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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] Ausencia de Content-Security-Policy: Facilita la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).

[HIGH] Falta de X-Frame-Options: Permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking para engañar usuarios.
[HIGH] Sin Strict-Transport-Security (HSTS): El servidor no obliga al navegador a usar siempre conexiones seguras, exponiendo el tráfico a interceptaciones.
[HIGH] Fallo en redirección HTTP a HTTPS: Las conexiones no seguras no se elevan automáticamente a protocolos cifrados de forma efectiva.
[MEDIUM] X-Content-Type-Options ausente: Permite que el navegador intente interpretar archivos con formatos incorrectos, aumentando el riesgo de ejecución de malware.
[MEDIUM] Referrer-Policy no configurado: No se controla la información de navegación que se envía a terceros al hacer clic en enlaces externos.
[MEDIUM] Permissions-Policy faltante: El sitio no restringe el uso de funciones sensibles del navegador como la cámara, el micrófono o la ubicación.
[MEDIUM] Archivos informativos accesibles: La presencia pública de /readme.html y /README.txt puede revelar detalles de la infraestructura a atacantes.
[MEDIUM] Bloqueo total en Robots.txt: La directiva Disallow: / impide el rastreo legítimo de buscadores y puede ocultar una estructura de directorios deficiente.
[MEDIUM] Puerto 8080 abierto: La exposición del puerto HTTP-Alt sugiere servicios adicionales que podrían no estar debidamente protegidos.
[LOW] Server header expuesto: Revela el uso de Cloudflare, proporcionando información útil para la fase de reconocimiento de un atacante.
[LOW] X-Powered-By expuesto: Indica el uso del framework Next.js, lo que permite dirigir ataques específicos contra esta tecnología.