EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://monitoreoyevaluacion.com	Checks	9 pruebas
Dominio	monitoreoyevaluacion.com	Hallazgos	44 totales
Fecha	21 de abril de 2026 a las 16:07	Problemas	10 detectados

B

77/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis técnico de ciberseguridad realizado al sitio web ha resultado en una puntuación de 77/100, obteniendo una nota final de B. Durante la auditoría se ejecutaron un total de 9 checks pasivos, obteniendo 6 resultados satisfactorios, una advertencia y dos fallos críticos en la configuración del servidor. Si bien el cifrado de datos es correcto, se detectó una carencia casi total de cabeceras de seguridad esenciales y la falta de políticas de transporte estricto. La ausencia de un pentest activo limita la visibilidad sobre vulnerabilidades lógicas, pero los datos actuales permiten concluir que el sitio es vulnerable a ataques de clickjacking y suplantación de identidad debido a configuraciones incompletas. Se requiere una intervención técnica inmediata para mitigar los riesgos identificados en las capas de transporte y respuesta.

Resumen de Riesgos

0	3	3	4	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 89 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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 89 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  89 dias restantes (expira: 2026-07-19T15:47:49.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-20T15:47:50.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: hcdn — Revela tecnologia del servidor
- BAJO **X-Powered-By expuesto**
  X-Powered-By: Next.js — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- 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://monitoreoyevaluacion.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

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

- 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 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea embebido en marcos de otras webs, facilitando ataques de clickjacking donde un atacante induce al usuario a realizar acciones involuntarias.

[HIGH] Strict-Transport-Security: No existe una política HSTS configurada, lo que permite que un atacante degrade la conexión de HTTPS a HTTP para interceptar datos sensibles en ataques de hombre en el medio (MITM).
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite al navegador intentar adivinar el tipo de contenido (MIME-sniffing), lo que puede ser explotado para ejecutar scripts maliciosos disfrazados de archivos estáticos.
[MEDIUM] Referrer-Policy: No se ha definido una política de referencia, lo que puede provocar la fuga de información sensible contenida en las URLs hacia sitios externos cuando un usuario hace clic en un enlace.
[MEDIUM] Permissions-Policy: El sitio no restringe el uso de APIs del navegador como la cámara o el micrófono, aumentando el riesgo en caso de que se logre inyectar código malicioso en el cliente.
[LOW] Server header expuesto: El servidor revela el valor hcdn, lo que facilita a un atacante identificar la infraestructura subyacente para buscar vulnerabilidades específicas.
[LOW] X-Powered-By expuesto: Se revela el uso del framework Next.js, información que ayuda a los atacantes a perfilar la tecnología del sitio y dirigir ataques contra debilidades conocidas de dicha versión.
[LOW] Robots.txt y Sitemap ausentes: La falta de estos archivos dificulta la correcta indexación y puede indicar una gestión de archivos en el servidor poco rigurosa o incompleta.