EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.elheraldo.hn/	Checks	9 pruebas
Dominio	www.elheraldo.hn	Hallazgos	54 totales
Fecha	20 de mayo de 2026 a las 21:43	Problemas	17 detectados

C

66/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio elheraldo.hn ha resultado en una puntuación de 66/100 y una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, se emitió 1 advertencia y se identificaron 3 fallos críticos de seguridad. Aunque la implementación del certificado SSL es correcta, se han detectado debilidades severas en la protección de cookies y el uso de software de gestión de contenidos desactualizado. Debido a la exposición de una versión antigua del CMS y la ausencia de cabeceras de seguridad esenciales, el sitio se considera vulnerable ante ataques dirigidos y requiere intervención inmediata.

Resumen de Riesgos

0	9	7	1	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 175 dias
Cabeceras de Seguridad	40	FALLO	Solo 2/6 presentes. Faltan: Strict-Transport-Sec...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 3.4.4 expuesta
Seguridad de Cookies	0	FALLO	ITR_COOKIE_DEVID: falta HttpOnly; ITR_COOKIE_DEV...
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	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 175 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  175 dias restantes (expira: 2026-11-11T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-11-11T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 40/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx/1.14.0 — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: frame-ancestors 'none';
- INFO **X-Frame-Options**
  Presente: DENY
- 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://www.elheraldo.hn/
- 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

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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, Astro

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 3.4.4 expuesta

- ALTO **WordPress version**
  Version 3.4.4 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)

Seguridad de Cookies — 0/100

Estado: FALLO

ITR_COOKIE_DEVID: falta HttpOnly; ITR_COOKIE_DEVID: falta Secure; ITR_COOKIE_DEVID: falta SameSite; ITR_COOKIE_USRID: falta HttpOnly;

ITR_COOKIE_USRID: falta Secure; ITR_COOKIE_USRID: falta SameSite; ITERWEBGEO: falta HttpOnly; ITERWEBGEO: falta Secure; ITERWEBGEO: falta SameSite

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- ALTO **Cookie: ITR_COOKIE_DEVID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: ITR_COOKIE_DEVID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: ITR_COOKIE_DEVID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: ITR_COOKIE_USRID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: ITR_COOKIE_USRID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: ITR_COOKIE_USRID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: ITERWEBGEO — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: ITERWEBGEO — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: ITERWEBGEO — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 (2968 bytes)
- INFO **Reglas robots.txt**
  93 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://www.elheraldo.hn/sitemap.xml
- 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

[LOW] Server header expuesto: El servidor revela el uso de nginx/1.14.0, facilitando a posibles atacantes la búsqueda de debilidades específicas para esa tecnología.
[HIGH] Strict-Transport-Security: La falta de la cabecera HSTS impide que el navegador fuerce conexiones cifradas, permitiendo posibles ataques de degradación de protocolo.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador podría intentar interpretar el contenido de forma distinta a la declarada, facilitando ataques de MIME-sniffing.
[MEDIUM] Referrer-Policy: La ausencia de esta política puede provocar que información sensible de la URL sea enviada a sitios externos mediante las cabeceras de referer.
[MEDIUM] Permissions-Policy: No se restringe el acceso de las APIs del navegador a funciones como la cámara o el micrófono, aumentando la superficie de riesgo para el usuario.
[HIGH] WordPress version: Se detectó la versión 3.4.4 expuesta públicamente, la cual es extremadamente antigua y vulnerable a múltiples exploits conocidos (CVEs).
[HIGH] Cookie ITR_COOKIE_DEVID: Carece de los flags HttpOnly y Secure, lo que permite su robo mediante ataques XSS y su transmisión en conexiones no seguras.
[MEDIUM] Cookie ITR_COOKIE_DEVID: Falta el atributo SameSite, dejando al sitio expuesto a ataques de falsificación de solicitud en sitios cruzados (CSRF).
[HIGH] Cookie ITR_COOKIE_USRID: No implementa HttpOnly ni Secure, permitiendo el acceso de scripts maliciosos a datos de sesión del usuario.
[MEDIUM] Cookie ITR_COOKIE_USRID: No utiliza el atributo SameSite para restringir el contexto de envío de la cookie.
[HIGH] Cookie ITERWEBGEO: Falta de protecciones HttpOnly y Secure, lo que compromete la integridad y privacidad de la información de geolocalización.
[MEDIUM] Cookie ITERWEBGEO: La ausencia de SameSite incrementa la vulnerabilidad ante ataques de tipo CSRF.
[MEDIUM] Bloqueo en robots.txt: El archivo bloquea la indexación de todo el sitio con la directiva Disallow: /, lo que podría ser una configuración incorrecta del sistema.