EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://elhubdeseguridad.com/	Checks	9 pruebas
Dominio	elhubdeseguridad.com	Hallazgos	51 totales
Fecha	9 de septiembre de 2026 a las 22:26	Problemas	10 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad del sitio elhubdeseguridad.com ha resultado en una puntuación de 70/100, lo que otorga una nota de C. Se han ejecutado un total de 9 comprobaciones pasivas, de las cuales 4 resultaron correctas, 4 generaron advertencias y 1 fue calificada como fallo crítico. Los hallazgos principales revelan una carencia importante de cabeceras de seguridad esenciales y una gestión de cookies que compromete la sesión del usuario. Aunque el sitio no utiliza un CMS conocido con vulnerabilidades públicas, las debilidades en la configuración del servidor y el transporte de datos son evidentes. En conclusión, el sitio se considera vulnerable a ataques de intermediario y de inyección debido a la falta de políticas de seguridad modernas.

Resumen de Riesgos

0	5	3	2	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	70	AVISO	Certificado expira en 16 dias
Cabeceras de Seguridad	30	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
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	67	AVISO	XSRF-TOKEN: falta HttpOnly; el_hub_de_seguridad_...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 70/100

Estado: AVISO

Certificado expira en 16 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- MEDIO **Dias hasta expiracion**
  16 dias restantes (expira: 2026-09-26T08:39:52.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-28T08:39:53.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 30/100

Estado: FALLO

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

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://elhubdeseguridad.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

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 — 67/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly; el_hub_de_seguridad_session: falta Secure

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: el_hub_de_seguridad_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: el_hub_de_seguridad_session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: el_hub_de_seguridad_session — SameSite**
  SameSite=lax

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 (107 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://elhubdeseguridad.com/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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 ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso en el navegador del usuario.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones cifradas, facilitando ataques de degradación de SSL.
[HIGH] Cookie XSRF-TOKEN: Falta el flag HttpOnly, lo que permite que la cookie sea accesible mediante scripts del lado del cliente, aumentando el riesgo de robo de identidad.
[HIGH] Cookie el_hub_de_seguridad_session: Falta el flag Secure, lo que provoca que la información de sesión se envíe por canales no cifrados si el usuario accede por HTTP.
[MEDIUM] Puerto 22 (SSH) abierto: El puerto de acceso remoto está expuesto a internet, lo que representa un punto de entrada potencial para ataques de fuerza bruta.
[MEDIUM] Referrer-Policy: La falta de esta política puede filtrar información sensible sobre el origen de la navegación a dominios externos.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente el acceso no autorizado a hardware como cámara o micrófono.
[LOW] Certificado SSL/TLS: El certificado digital expira en 16 días, lo que compromete la disponibilidad de la conexión segura a corto plazo.
[LOW] Server header expuesto: La cabecera revela el uso de nginx, lo que facilita a un atacante la identificación de la tecnología y la búsqueda de exploits específicos.
[LOW] Ruta sensible en robots.txt: Se referencia la ruta admin, lo que expone la ubicación de posibles paneles de gestión a recolectores de información.