

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://lahaineerotic.com
Dominio lahaineerotic.com
Fecha 8 de octubre de 2026 a las 00:15

Checks 9 pruebas
Hallazgos 42 totales
Problemas 7 detectados

C

70/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad del sitio web arroja una puntuación de 70/100, lo que equivale a una nota de C. Se han completado un total de 9 comprobaciones pasivas, identificando 5 resultados satisfactorios, 2 advertencias y 2 fallos críticos en la configuración del servidor. Aunque la transmisión de datos posee un certificado válido, la ausencia de redirecciones forzadas y cabeceras de seguridad debilita la postura defensiva. En su estado actual, se concluye que el sitio es vulnerable debido a configuraciones de red incompletas y exposición de puertos innecesarios.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 60 dias
Cabeceras de Seguridad	65	AVISO	4/6 presentes. Faltan: Strict-Transport-Security...
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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 60 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
60 dias restantes (expira: 2026-12-06T18:17:18.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-07T17:17:21.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 65/100

Estado: AVISO

4/6 presentes. Faltan: Strict-Transport-Security, X-Content-Type-Options

- BAJO Server header expuesto
Server: cloudflare — 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
- INFO

Referrer-Policy
Presente: no-referrer
- INFO

Permissions-Policy
Presente: display-capture=()

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO

HTTP !' HTTPS redireccion
HTTP 200 — 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

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

sitemap.xml

No encontrado (HTTP 404)

BAJO

security.txt

No encontrado — Recomendado para politica de divulgacion

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] HTTP ! HTTPS redireccion: El servidor permite el acceso mediante HTTP sin redirigir automáticamente a la versión cifrada, dejando el tráfico expuesto.

[HIGH] Strict-Transport-Security (HSTS): La ausencia de esta cabecera impide que el navegador obligue siempre el uso de conexiones HTTPS seguras.

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este puerto alternativo puede ser utilizada para servicios no supervisados o ataques de proxy.

[MEDIUM] X-Content-Type-Options: Falta la cabecera que previene al navegador de interpretar archivos como un tipo MIME diferente al declarado, evitando ataques de inyección.

[LOW] Server header expuesto: Se revela el uso de tecnología Cloudflare, lo cual facilita a un atacante potencial el reconocimiento de la infraestructura.

[LOW] sitemap.xml: El archivo de mapa del sitio no fue localizado, lo que indica una gestión de recursos web incompleta.