EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ultimashoras.com	Checks	9 pruebas
Dominio	ultimashoras.com	Hallazgos	48 totales
Fecha	20 de mayo de 2026 a las 02:06	Problemas	9 detectados

B

79/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del dominio ultimashoras.com ha dado como resultado una puntuación de 79/100, lo que se traduce en una nota de B. Durante la auditoría se realizaron 9 checks pasivos, logrando 6 resultados satisfactorios, 2 advertencias y 1 fallo crítico en la configuración de cabeceras. Aunque el sitio cuenta con un cifrado SSL robusto, la falta de protecciones contra ataques de clickjacking y degradación de protocolos aumenta el riesgo para el usuario final. Se concluye que el sitio es moderadamente seguro, pero presenta vulnerabilidades técnicas que deben ser mitigadas para alcanzar un estándar profesional de protección web.

Resumen de Riesgos

0	3	3	3	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 78 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	1 cookies, todas con flags correctos
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 78 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  78 dias restantes (expira: 2026-08-06T00:20:26.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-08T00:20:27.000Z
- 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: PHP/8.2.30 — 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://ultimashoras.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**
  PHP/8.2.30

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

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: _csrf-frontend — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: _csrf-frontend — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _csrf-frontend — 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (22 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 1 Allow
- 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] Falta de X-Frame-Options: No se detectó esta cabecera, lo que permite que el sitio sea embebido en frames externos facilitando ataques de clickjacking donde se engaña al usuario para que haga clic en elementos invisibles.
[HIGH] Falta de Strict-Transport-Security: La ausencia de HSTS impide que el navegador fuerce siempre una conexión HTTPS, permitiendo posibles ataques de degradación de SSL (SSL Strip).
[MEDIUM] Falta de X-Content-Type-Options: Sin esta cabecera, los navegadores podrían intentar adivinar el tipo de contenido (MIME-sniffing), lo que puede llevar a la ejecución involuntaria de scripts maliciosos ocultos en archivos de texto o imágenes.
[MEDIUM] Falta de Referrer-Policy: No existe control sobre la información de origen que se envía a otros sitios cuando el usuario hace clic en un enlace, lo que podría filtrar URLs privadas o datos de navegación.
[MEDIUM] Falta de Permissions-Policy: El sitio no restringe el acceso a funciones del navegador como la cámara, el micrófono o la geolocalización, aumentando la superficie de ataque en caso de una intrusión.
[LOW] Cabecera Server expuesta: Se revela el valor hcdn, lo cual entrega pistas innecesarias sobre la infraestructura y tecnología del servidor a potenciales atacantes.
[LOW] Cabecera X-Powered-By expuesta: Se muestra explícitamente el uso de PHP/8.2.30, permitiendo que atacantes busquen vulnerabilidades específicas para esa versión exacta del lenguaje.
[LOW] Ausencia de sitemap.xml: No se encontró el archivo de mapa del sitio, lo cual es una deficiencia menor de cara a la indexación y visibilidad de la estructura del portal.