EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cuevana.gs/	Checks	9 pruebas
Dominio	cuevana.gs	Hallazgos	45 totales
Fecha	20 de mayo de 2026 a las 21:31	Problemas	13 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado a la plataforma arroja una puntuación de 64/100, lo que equivale a una nota de C. Durante la evaluación técnica, se ejecutaron 9 checks pasivos, resultando en 5 satisfactorios, 2 advertencias y 2 fallos críticos relacionados con la configuración del servidor. Aunque la gestión del certificado SSL es correcta, la ausencia total de cabeceras de seguridad y la exposición de versiones específicas del CMS representan un riesgo significativo para la integridad del sitio. Debido a estas deficiencias técnicas y la falta de mecanismos de endurecimiento, se concluye que el sitio web se encuentra en un estado vulnerable frente a ataques automatizados y de inyección.

Resumen de Riesgos

0	5	6	2	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 79 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 6.9.4 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
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): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 79 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  79 dias restantes (expira: 2026-08-07T20:20:15.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-09T20:20:16.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- 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://cuevana.gs/
- 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
- BAJO **Meta generator**
  Expone: WordPress 6.9.4

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.9.4 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (1906 bytes)
- INFO **Reglas robots.txt**
  10 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://cuevana.gs/sitemap_index.xml
- 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] Content-Security-Policy: Falta esta cabecera, lo que facilita ataques de ejecución de scripts cruzados (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: No configurada, permitiendo que el sitio sea embebido en marcos externos, lo que habilita ataques de clickjacking.
[HIGH] Strict-Transport-Security: Ausencia de HSTS, lo que impide que el navegador fuerce conexiones seguras y deja la sesión expuesta a ataques de degradación de protocolo.

[HIGH] WordPress version: La versión 6.9.4 está expuesta públicamente, permitiendo a potenciales atacantes identificar y explotar CVEs conocidos para esa versión.
[MEDIUM] X-Content-Type-Options: Falta la directiva, permitiendo que el navegador intente adivinar el tipo de contenido (MIME-sniffing), lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No definida, lo que compromete la privacidad al no controlar qué información de referencia se envía a otros dominios.
[MEDIUM] Permissions-Policy: Falta, permitiendo que el sitio acceda potencialmente a APIs del navegador sin restricciones de seguridad.
[MEDIUM] Archivo /readme.html: Accesible de forma pública, lo cual es una mala práctica que revela información técnica del motor del sitio.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó este puerto abierto, lo que aumenta la superficie de ataque al exponer un servicio web alternativo o proxy.
[MEDIUM] Bloqueo total en robots.txt: La directiva Disallow bloquea todo el sitio, lo cual puede indicar una configuración incorrecta de visibilidad o un intento rudimentario de ocultación.
[LOW] Server header expuesto: Revela el uso de Cloudflare, proporcionando pistas sobre la infraestructura de red a actores externos.
[LOW] Meta generator: El código fuente expone la versión exacta del CMS, facilitando la labor de reconocimiento del atacante.