EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cuevana3.pub/	Checks	9 pruebas
Dominio	cuevana3.pub	Hallazgos	47 totales
Fecha	20 de mayo de 2026 a las 21:32	Problemas	15 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar la auditoría técnica a la infraestructura web, el sitio obtuvo una puntuación de 72/100 con una calificación de grado C. Los análisis pasivos consistieron en 9 verificaciones, de las cuales 6 resultaron satisfactorias, 2 generaron advertencias y 1 fue categorizada como fallo crítico. Se identificó una ausencia total de cabeceras de seguridad fundamentales y configuraciones deficientes en la persistencia de la conexión cifrada. Debido a estas omisiones en la protección del servidor y del navegador, el sitio se considera vulnerable a ataques de inyección de código y suplantación.

Resumen de Riesgos

0	4	10	1	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 84 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	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	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 84 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  84 dias restantes (expira: 2026-08-13T01:49:57.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-15T01:49:58.000Z
- 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://cuevana3.pub/
- 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

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente

- 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (502 bytes)
- INFO **Reglas robots.txt**
  12 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **sitemap.xml**
  Presente, 1 URLs
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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: La ausencia de esta cabecerda facilita ataques de Cross-Site Scripting (XSS) e inyección de datos maliciosos.
[HIGH] X-Frame-Options: La falta de esta protección permite que el sitio sea cargado en marcos externos, elevando el riesgo de ataques de Clickjacking.
[HIGH] Strict-Transport-Security: No está configurada, lo que impide que el navegador fuerce siempre una conexión segura HTTPS a través de HSTS.
[MEDIUM] X-Content-Type-Options: La omisión de esta cabecera permite el MIME-type sniffing, lo que puede derivar en la ejecución de scripts no autorizados.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a dominios externos durante la navegación.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, dejando expuestos accesos potenciales a funciones como cámara o micrófono.
[MEDIUM] Puerto 8080 (HTTP-Alt): Este puerto se encuentra abierto, lo que representa una superficie de ataque adicional en un servicio no estándar.
[MEDIUM] Archivos informativos expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, pudiendo revelar detalles técnicos del entorno.
[MEDIUM] Rutas de administración accesibles: Se detectaron puntos de entrada como /wp-login.php y /administrator/ expuestos sin restricciones perimetrales.
[LOW] Server header expuesto: La cabecera revela el uso de tecnología Cloudflare, proporcionando información sobre la arquitectura de red a posibles atacantes.