EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.cinecalidad.am/	Checks	9 pruebas
Dominio	www.cinecalidad.am	Hallazgos	46 totales
Fecha	20 de mayo de 2026 a las 21:26	Problemas	14 detectados

D

53/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada sobre el sitio web ha arrojado una puntuación de 53/100, resultando en una calificación de nota D. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 fueron satisfactorios, 1 presentó advertencias y 3 fallaron debido a configuraciones críticas omitidas. El análisis revela deficiencias severas en la implementación de cabeceras de seguridad y en la gestión de protocolos de cifrado, a pesar de contar con un certificado SSL válido. La exposición pública de versiones del software y la falta de redirecciones forzosas aumentan significativamente la superficie de ataque. En conclusión, el sitio se considera vulnerable y requiere atención inmediata para mitigar riesgos de interceptación y manipulación de datos.

Resumen de Riesgos

0	6	6	2	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 46 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.6.5 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 46 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  46 dias restantes (expira: 2026-07-05T18:02:27.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-06T17:03:57.000Z
- 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 — 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

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.6.5
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.6.5 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.6.5 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 (2027 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://www.cinecalidad.ec/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] Falta de cabecera Content-Security-Policy: La ausencia de CSP permite la ejecución de scripts no autorizados y ataques de inyección de contenido XSS.
[HIGH] Falta de cabecera X-Frame-Options: La web es vulnerable a ataques de clickjacking al no restringir cómo se carga el sitio en marcos o iframes.
[HIGH] Falta de cabecera Strict-Transport-Security: No se comunica al navegador que debe usar exclusivamente conexiones HTTPS, permitiendo ataques de degradación.
[HIGH] Sin redirección HTTP a HTTPS: El sitio responde con un código 200 en conexiones no cifradas, exponiendo los datos transmitidos por los usuarios.
[HIGH] Exposición de versión de WordPress 6.6.5: Revelar la versión exacta del CMS permite a potenciales atacantes identificar y explotar CVEs conocidos.
[MEDIUM] Falta de cabecera X-Content-Type-Options: La ausencia de esta directiva facilita ataques de sniffing de tipos MIME para ejecutar archivos maliciosos.
[MEDIUM] Falta de cabecera Referrer-Policy: No existe control sobre la información de referencia enviada a otros dominios, comprometiendo la privacidad de la navegación.
[MEDIUM] Falta de cabecera Permissions-Policy: No se restringe el acceso del navegador a funciones sensibles como la cámara, el micrófono o la ubicación.
[MEDIUM] Archivo /readme.html accesible: Este archivo público puede filtrar detalles técnicos sobre la instalación y versiones del gestor de contenidos.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de puertos alternativos aumenta los puntos de entrada potenciales para escaneos y ataques dirigidos.
[MEDIUM] Bloqueo total en robots.txt: La configuración Disallow: / bloquea toda la indexación, lo cual puede ser un error de visibilidad o una medida defensiva mal aplicada.
[LOW] Cabecera Server expuesta: Se identifica el uso de Cloudflare, lo que proporciona información sobre la infraestructura tecnológica a terceros.
[LOW] Exposición de Meta generator: La etiqueta meta en el código fuente confirma el uso de WordPress 6.6.5, facilitando el reconocimiento del objetivo.