EscanearVulnerabilidades

Informe de Seguridad Web

URL	http://ww17.cinecalidad.bar/	Checks	9 pruebas
Dominio	ww17.cinecalidad.bar	Hallazgos	44 totales
Fecha	20 de mayo de 2026 a las 21:32	Problemas	16 detectados

D

51/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al sitio web arroja una puntuación de 51/100, lo que equivale a una nota D. Durante la auditoría se ejecutaron 9 checks pasivos, resultando en 4 verificaciones correctas, 2 advertencias por configuraciones incompletas y 2 fallos críticos en la infraestructura base. El sitio carece de mecanismos esenciales de cifrado y protección contra ataques comunes de interceptación. Debido a la ausencia de certificados de seguridad válidos y la falta total de cabeceras de protección, se concluye que el sitio es actualmente vulnerable y no es seguro para el intercambio de información.

Resumen de Riesgos

1	5	9	1	28
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	50	AVISO	El sitio no usa HTTPS, no aplica chequeo de cont...
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 0/100

Estado: FALLO

Certificado SSL no valido

- CRITICO **Certificado valido**
  El certificado SSL NO es valido
- INFO **Dias hasta expiracion**
  1471 dias restantes (expira: 2030-05-31T05:41:49.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2020-06-02T05:41:49.000Z
- 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: nginx/1.28.0 — 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: ERROR

No se pudo verificar la redireccion HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS

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 — 50/100

Estado: AVISO

El sitio no usa HTTPS, no aplica chequeo de contenido mixto

- ALTO **Protocolo**
  El sitio no usa HTTPS

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (292 bytes)
- INFO **Reglas robots.txt**
  10 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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

[CRITICAL] Certificado SSL no válido: El sitio no cuenta con un certificado SSL funcional, impidiendo el cifrado de la conexión.
[HIGH] HTTP a HTTPS redirección fallida: El servidor no redirige el tráfico inseguro a una conexión cifrada, manteniendo el puerto 80 abierto sin protección.
[HIGH] Content-Security-Policy faltante: La ausencia de esta política permite ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options faltante: El sitio es vulnerable a ataques de clickjacking al permitir ser embebido en marcos externos sin restricciones.
[HIGH] Strict-Transport-Security faltante: No se instruye al navegador para usar exclusivamente conexiones HTTPS, facilitando ataques de degradación de SSL.

[MEDIUM] X-Content-Type-Options faltante: La falta de esta cabecera permite que el navegador realice MIME-sniffing, aumentando el riesgo de ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy faltante: No se controla la información de procedencia enviada a otros sitios, lo que puede comprometer la privacidad de la navegación.
[MEDIUM] Permissions-Policy faltante: El servidor no restringe el uso de APIs del navegador como la cámara, el micrófono o la ubicación.
[MEDIUM] Archivos sensibles expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente y pueden revelar detalles técnicos del sistema.
[MEDIUM] Rutas administrativas descubiertas: Los endpoints /wp-login.php, /administrator/ y /user/login están expuestos a intentos de acceso no autorizados.
[MEDIUM] Bloqueo en robots.txt: El archivo de configuración bloquea el rastreo de todo el sitio, lo que puede ocultar estructuras mal configuradas.
[LOW] Server header expuesto: El servidor revela el uso de nginx/1.28.0, facilitando a potenciales atacantes la búsqueda de vulnerabilidades específicas para esa versión.