EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://arteymanos.cl/	Checks	9 pruebas
Dominio	arteymanos.cl	Hallazgos	51 totales
Fecha	6 de agosto de 2026 a las 12:32	Problemas	7 detectados

B

89/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web arteymanos.cl ha resultado en una puntuación de 89/100 con una nota B. Se ejecutaron un total de 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 presentaron fallos técnicos. Aunque la infraestructura de cifrado y las cabeceras de seguridad son sólidas, se detectaron vulnerabilidades en la gestión de cookies de sesión. Se concluye que el sitio es generalmente seguro, pero presenta debilidades específicas que podrían ser explotadas para comprometer las sesiones de los usuarios.

Resumen de Riesgos

0	2	2	3	44
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 55 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	33	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Same...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 55 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  55 dias restantes (expira: 2026-09-30T04:34:26.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-02T04:34:27.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

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

- INFO **Content-Security-Policy**
  Presente: default-src 'self' https: data: blob:; img-src 'self' https: data: blob:; script...
- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(), camera=(), microphone=(), payment=(), usb=(), bluetooth=(), acce...

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://arteymanos.cl/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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**
  Next.js

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 — 33/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta SameSite; visita_registrada: falta HttpOnly; visita_registrada: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: PHPSESSID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: visita_registrada — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: visita_registrada — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: visita_registrada — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- 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] Cookie PHPSESSID sin HttpOnly: La ausencia de este atributo permite que la cookie sea accesible mediante scripts del lado del cliente, aumentando el riesgo de robo de sesión ante ataques XSS.
[HIGH] Cookie visita_registrada sin HttpOnly: Esta cookie de sesión carece de protección contra acceso programático, lo que compromete la integridad de la navegación del usuario.
[MEDIUM] Cookie PHPSESSID sin SameSite: La falta de esta directiva hace que la sesión sea vulnerable a ataques de falsificación de solicitudes en sitios cruzados o CSRF.
[MEDIUM] Cookie visita_registrada sin SameSite: Al no definir una política de sitio cruzado, el navegador podría enviar esta cookie en peticiones originadas desde dominios externos maliciosos.
[LOW] Cabecera Server expuesta: Se detectó el valor Server: hcdn, lo cual revela información sobre la tecnología de entrega de contenido y facilita el reconocimiento para atacantes.
[LOW] Ausencia de robots.txt: No se encontró el archivo de instrucciones para rastreadores, lo que afecta la gestión de acceso a directorios del sitio.
[LOW] Ausencia de sitemap.xml: El sitio carece de un mapa de estructura web, dificultando la indexación correcta y la visibilidad de su jerarquía de archivos.