EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.cndh.org.mx	Checks	9 pruebas
Dominio	www.cndh.org.mx	Hallazgos	49 totales
Fecha	12 de mayo de 2026 a las 16:52	Problemas	16 detectados

C

67/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio cndh.org.mx arroja una puntuación de 67/100, lo que equivale a una nota de C. Se ejecutaron 9 checks pasivos, resultando en 4 verificaciones exitosas, 2 advertencias por configuraciones incompletas y 3 fallos críticos en parámetros de seguridad esenciales. Aunque el cifrado base es correcto, la ausencia de cabeceras de protección y deficiencias en la gestión de cookies elevan el riesgo técnico. En su estado actual, el sitio se considera vulnerable a ataques de intermediario e inyección de código debido a una configuración de servidor permisiva.

Resumen de Riesgos

0	4	10	2	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 116 dias
Cabeceras de Seguridad	30	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: Drupal
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	33	FALLO	cookiesession1: falta Secure; cookiesession1: fa...
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 116 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  116 dias restantes (expira: 2026-09-05T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-09-04T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 30/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Microsoft-IIS/10.0 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://www.cndh.org.mx:443/
- 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: Drupal

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  Detectado via HTML body
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  ASP.NET

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 — 33/100

Estado: FALLO

cookiesession1: falta Secure; cookiesession1: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: cookiesession1 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: cookiesession1 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: cookiesession1 — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://appweb.cndh.org.mx/biblioteca/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://appweb.cndh.org.mx/contrataciones/

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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] Content-Security-Policy faltante: La ausencia de esta cabecera permite la ejecución de scripts no autorizados y ataques de inyección de contenido.
[HIGH] Strict-Transport-Security (HSTS) no configurado: El servidor no obliga al navegador a usar conexiones seguras, permitiendo ataques de degradación de SSL.
[HIGH] Cookie insegura (cookiesession1): La cookie carece del flag Secure, lo que permite que sea transmitida a través de conexiones HTTP no cifradas.
[MEDIUM] Cookie sin atributo SameSite: La cookie cookiesession1 es vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido mixto detectado: Se identificaron recursos cargados mediante HTTP (biblioteca y contrataciones) dentro de una página HTTPS, comprometiendo la integridad del sitio.
[MEDIUM] Archivos informativos expuestos: El acceso público a /readme.html y /README.txt facilita la obtención de metadatos técnicos sobre el CMS Drupal.
[MEDIUM] Paneles de gestión accesibles: Rutas críticas como /user/login y otros endpoints de administración están expuestos a intentos de acceso no autorizado.
[MEDIUM] Referrer-Policy y Permissions-Policy faltantes: No existe control sobre la información de navegación compartida ni sobre el uso de APIs del navegador.
[LOW] Cabeceras de tecnología expuestas: El servidor revela el uso de Microsoft-IIS/10.0 y ASP.NET, lo cual asiste a atacantes en la fase de reconocimiento.
[LOW] Ausencia de robots.txt y sitemap.xml: El sitio carece de archivos de control para rastreadores, afectando la visibilidad y el orden de indexación.