EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://coopdgii.com	Checks	9 pruebas
Dominio	coopdgii.com	Hallazgos	50 totales
Fecha	25 de septiembre de 2026 a las 17:45	Problemas	21 detectados

D

47/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio coopdgii.com muestra un desempeño deficiente con una puntuación de 47/100 y una calificación de nota D. Se ejecutaron 9 checks pasivos que resultaron en solo 2 verificaciones correctas, 3 advertencias y 4 fallos de seguridad críticos. Los hallazgos revelan la falta total de cabeceras de protección, exposición de versiones de software y servicios de base de datos accesibles desde internet. Se concluye que el sitio es actualmente vulnerable y presenta vectores de ataque de alto impacto que comprometen la integridad de la infraestructura.

Resumen de Riesgos

2	7	8	4	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 35 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	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 7.1.2 expuesta, WordPress 2 expuesta
Seguridad de Cookies	33	FALLO	nfd-enable-cf-opt: falta Secure; nfd-enable-cf-o...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	20	FALLO	4 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 35 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  35 dias restantes (expira: 2026-10-30T13:24:38.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-01T13:24:39.000Z
- 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/1.29.8 — 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://coopdgii.com/
- 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 7.1.2
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.1.2 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.1.2 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)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

Seguridad de Cookies — 33/100

Estado: FALLO

nfd-enable-cf-opt: falta Secure; nfd-enable-cf-opt: falta SameSite

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

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://coopdgii.com/coopvirtual/login

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (67 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

4 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — 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] Puerto 3306 (MySQL) abierto: La base de datos se encuentra expuesta públicamente, permitiendo intentos de conexión externa y ataques de fuerza bruta.
[CRITICAL] Puerto 5432 (PostgreSQL) abierto: El servicio de base de datos está accesible desde cualquier ubicación en internet, lo que supone un riesgo de filtración masiva de datos.
[HIGH] Cabeceras de seguridad ausentes: El sitio no implementa ninguna de las 6 cabeceras esenciales (CSP, HSTS, X-Frame-Options, etc.), dejando a los usuarios desprotegidos ante ataques XSS y clickjacking.
[HIGH] Versión de CMS expuesta: Se detectó públicamente el uso de WordPress 7.1.2 y WordPress 2, lo que permite a los atacantes identificar y explotar vulnerabilidades conocidas para esas versiones.
[HIGH] Puerto 21 (FTP) abierto: Este servicio transfiere información sin cifrado, lo que puede permitir la interceptación de credenciales de administración.
[HIGH] HSTS no configurado: El servidor no fuerza el uso de HTTPS, facilitando ataques de degradación de protocolo (SSL Stripping).
[HIGH] Cookie sin flag Secure: La cookie nfd-enable-cf-opt se transmite por canales no cifrados, permitiendo su captura en redes públicas.
[MEDIUM] Falta de flag SameSite en cookies: La ausencia de este atributo en nfd-enable-cf-opt hace que el sitio sea susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido mixto: El recurso http://coopdgii.com/coopvirtual/login se carga mediante una conexión no segura dentro de un entorno HTTPS.
[MEDIUM] Puerto 22 (SSH) abierto: El acceso remoto al servidor está expuesto, lo que incrementa la superficie de ataque para intrusiones a nivel de sistema operativo.
[MEDIUM] Archivos y rutas sensibles expuestas: El acceso público a /wp-login.php y /readme.html facilita el reconocimiento de la infraestructura por parte de terceros.
[LOW] Server header expuesto: La cabecera revela el uso de nginx/1.29.8, brindando información técnica útil para planificar ataques dirigidos.
[LOW] Referencias administrativas en robots.txt: Se mencionan rutas sensibles como "admin", lo que guía a los atacantes hacia áreas restringidas del sitio.