EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://pntc.miambiente.gob.pa	Checks	9 pruebas
Dominio	pntc.miambiente.gob.pa	Hallazgos	51 totales
Fecha	10 de abril de 2026 a las 19:19	Problemas	10 detectados

B

78/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio pntc.miambiente.gob.pa arroja una puntuación de 78/100, lo que corresponde a una calificación de grado B. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 presentó advertencias y 2 fallaron significativamente. Si bien el sitio cuenta con un cifrado SSL robusto y una correcta redirección HTTPS, se detectaron deficiencias críticas en las cabeceras de seguridad y en la configuración de las cookies. Debido a la ausencia de políticas de seguridad de contenido y protecciones contra el secuestro de sesiones, el sitio se considera vulnerable ante ataques de inyección y manipulación de tráfico.

Resumen de Riesgos

0	3	5	2	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 32 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	33	FALLO	PHPSESSID: falta Secure; PHPSESSID: falta SameSi...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 32 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  32 dias restantes (expira: 2026-05-12T20:23:12.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-11T20:23:13.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache/2.4.62 (Debian) — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://pntc.miambiente.gob.pa/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains
- 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

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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

- 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 Secure; PHPSESSID: falta SameSite; sc_actual_lang_pntc: falta Secure; sc_actual_lang_pntc: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: PHPSESSID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: sc_actual_lang_pntc — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: sc_actual_lang_pntc — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: sc_actual_lang_pntc — 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (98 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 2 Allow
- 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] Content-Security-Policy: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso al no restringir las fuentes de recursos.
[HIGH] Cookie PHPSESSID (flag Secure): La falta del flag Secure permite que la cookie de sesión se envíe a través de conexiones HTTP no cifradas, facilitando la interceptación de la sesión.
[HIGH] Cookie sc_actual_lang_pntc (flag Secure): Esta cookie se transmite sin protección de cifrado, lo que expone datos de navegación en redes no seguras.
[MEDIUM] Cookie PHPSESSID (flag SameSite): Al carecer del flag SameSite, el sitio es susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Cookie sc_actual_lang_pntc (flag SameSite): La ausencia de esta restricción facilita que sitios externos puedan manipular o acceder a peticiones vinculadas a esta cookie.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido (MIME-sniffing), lo que puede derivar en la ejecución de scripts disfrazados.
[MEDIUM] Referrer-Policy: No se tiene control sobre la información de procedencia enviada a otros dominios, lo que podría filtrar URLs privadas o sensibles.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como la cámara o el micrófono, aumentando la superficie de ataque en el lado del cliente.
[LOW] Server header expuesto: El servidor responde con la firma Apache/2.4.62 (Debian), revelando versiones exactas del software y sistema operativo que pueden ser buscadas para exploits conocidos.
[LOW] sitemap.xml: El archivo no fue encontrado (404), lo que dificulta la indexación estructurada y el análisis de la arquitectura del sitio.