

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://difor.miambiente.gob.pa	Checks	9 pruebas
Dominio	difor.miambiente.gob.pa	Hallazgos	46 totales
Fecha	10 de abril de 2026 a las 19:25	Problemas	6 detectados

B

83/100

puntos de seguridad



RESUMEN EJECUTIVO

El sitio web difor.miambiente.gob.pa ha obtenido una puntuacion de 83/100 con una nota de B, lo que indica una postura de seguridad aceptable pero con deficiencias criticas que requieren atencion inmediata. El analisis se baso en 9 checks pasivos, de los cuales 6 resultaron exitosos, 1 presento advertencias y 2 fallaron significativamente. A pesar de contar con una base solida en cifrado y redirecciones, la exposicion de versiones obsoletas del CMS representa un riesgo elevado. Se concluye que el sitio es vulnerable debido a la falta de actualizacion de su nucleo y la ausencia de politicas de seguridad en cabeceras. La infraestructura actual es susceptible a ataques dirigidos si no se corrigen los hallazgos de versionamiento.

Resumen de Riesgos

0	2	0	4	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 87 dias
Cabeceras de Seguridad	75	AVISO	5/6 presentes. Faltan: Content-Security-Policy
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 1.3.7 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
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 87 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
87 dias restantes (expira: 2026-07-06T22:00:14.000Z)
- INFO Fecha de emision
Emitido desde: 2026-04-07T22:00:15.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

5/6 presentes. Faltan: Content-Security-Policy

- BAJO Server header expuesto
Server: nginx — Revela tecnologia del servidor

- ALTO

Content-Security-Policy
Falta — Previene XSS y ataques de inyeccion de contenido
- INFO

X-Frame-Options
Presente: DENY
- INFO

Strict-Transport-Security
Presente: max-age=63072000; 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=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://difor.miambiente.gob.pa/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=63072000; includeSubDomains; preload
- BAJO

HSTS includeSubDomains
HSTS cubre subdominios
- INFO

HSTS max-age
max-age=63072000 (730 dias)
- 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: Redux 4.5.11
- INFO

Tecnologias detectadas
Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 1.3.7 expuesta

- ALTO

WordPress version
Version 1.3.7 expuesta publicamente — Permite a atacantes buscar CVEs conocidos

- INFO

Archivo /readme.html
No accesible (correcto)
- INFO

Archivo /README.txt
No accesible (correcto)

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 — 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 autentificacion 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

[ALTA] WordPress version: La version 1.3.7 se encuentra expuesta publicamente, lo cual es critico ya que permite a atacantes identificar y explotar vulnerabilidades conocidas en versiones antiguas del software.

[ALTA] Content-Security-Policy: La ausencia de esta cabecera impide prevenir ataques de inyeccion de contenido como Cross-Site Scripting (XSS), dejando a los usuarios desprotegidos.

[BAJA] Server header expuesto: El servidor revela el uso de nginx, informacion que ayuda a posibles atacantes a perfilar la infraestructura tecnologica.

[BAJA] Meta generator: Se detecto la exposicion de Redux 4.5.11 a traves de etiquetas meta, facilitando el reconocimiento de componentes internos del sitio.

[BAJA] robots.txt: El archivo no fue encontrado (error 404), lo que puede afectar la indexacion y la gestion del trafico de rastreadores.

[BAJA] sitemap.xml: La ausencia de un mapa del sitio dificulta la visibilidad de la estructura de contenidos para herramientas de auditoria y motores de busqueda.