EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cuencas.miambiente.gob.pa	Checks	9 pruebas
Dominio	cuencas.miambiente.gob.pa	Hallazgos	49 totales
Fecha	10 de abril de 2026 a las 19:32	Problemas	9 detectados

B

77/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al dominio cuencas.miambiente.gob.pa arroja una puntuación de 77/100, lo que equivale a una calificación de nota B. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 se identificaron como fallos críticos. Aunque la infraestructura de cifrado y redirección es sólida, la exposición de versiones obsoletas y la falta de políticas de contenido representan un riesgo significativo. En su estado actual, el sitio se considera vulnerable debido a la presencia de fallos de severidad alta que podrían ser explotados por atacantes externos.

Resumen de Riesgos

0	2	4	3	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 4.12.7 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	6 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
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: 2026-07-06T21:59:35.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-07T21:59:36.000Z
- 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://cuencas.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: Elementor 4.0.1; features: additional_custom_breakpoints; settings: css_print_method-external, google_font-enabled, font_display-auto
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 4.12.7 expuesta

- ALTO **WordPress version**
  Version 4.12.7 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 — 20/100

Estado: FALLO

6 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://cuencas.miambiente.gob.pa/quienes-somos/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://cuencas.miambiente.gob.pa/leyes/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://cuencas.miambiente.gob.pa/resoluciones/
- MEDIO **href (link/stylesheet)**
  ...y 3 mas del mismo tipo

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta robots.txt

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- INFO **sitemap.xml**
  Presente, ? URLs
- 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] WordPress version: Versión 4.12.7 expuesta públicamente. Esta exposición permite a atacantes identificar y explotar CVEs conocidos asociados a una versión desactualizada del CMS.
[HIGH] Content-Security-Policy: Falta esta cabecera de seguridad. Su ausencia facilita la ejecución de ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[MEDIUM] Contenido Mixto: Se detectaron 6 recursos cargados a través de HTTP en una página protegida por HTTPS. Esto compromete la integridad del cifrado y puede permitir la interceptación de datos en tránsito.
[LOW] Server header expuesto: El servidor revela el uso de nginx. Esta información ayuda a los atacantes a perfilar la tecnología del servidor para buscar vulnerabilidades específicas de la plataforma.
[LOW] Meta generator: Se expone el uso de Elementor 4.0.1 y sus configuraciones internas. Revelar detalles de plugins y constructores visuales amplía la superficie de reconocimiento para un atacante.
[LOW] robots.txt: El archivo no fue encontrado (Error 404). Esto impide definir correctamente qué áreas del sitio deben o no ser indexadas por los motores de búsqueda.