EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://rutaportuaria.co/	Checks	9 pruebas
Dominio	rutaportuaria.co	Hallazgos	49 totales
Fecha	13 de abril de 2026 a las 19:25	Problemas	10 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web analizado presenta una puntuación de seguridad de 80/100, lo que le otorga una calificación de grado B. Tras ejecutar un total de 9 checks pasivos, se determinó que la mayoría de los parámetros de cifrado y cabeceras son correctos, aunque se identificaron 2 fallos críticos y una advertencia técnica. El entorno muestra una configuración robusta en su capa de transporte SSL, pero presenta debilidades severas en la exposición de servicios de infraestructura. Debido a la visibilidad pública de puertos críticos y versiones del software, el sitio se considera actualmente vulnerable ante ataques dirigidos de reconocimiento y explotación de servicios. Es imperativo corregir las brechas en el firewall para elevar el nivel de protección.

Resumen de Riesgos

1	2	4	3	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 77 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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 82 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 77 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  77 dias restantes (expira: 2026-06-29T20:54:58.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-31T20:54:59.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- BAJO **Server header expuesto**
  Server: LiteSpeed — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: default-src 'self' https: data: blob: 'unsafe-inline' 'unsafe-eval'; img-src 'se...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- 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=(), microphone=(), camera=(), usb=(), fullscreen=(self), payment=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://rutaportuaria.co/
- 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 4.0.2; 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 82 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 82 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)

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 — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://consulta.sfconvias.co
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://instagram.com/s.f.convias

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (117 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://rutaportuaria.co/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 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
- 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

[CRITICAL] Puerto 3306 (MySQL): El servicio de base de datos se encuentra abierto a internet, permitiendo intentos de conexión externa y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP): Este protocolo transfiere credenciales y datos en texto plano, lo que facilita la interceptación de información sensible por parte de terceros.
[HIGH] WordPress versión: La versión 82 del CMS está expuesta públicamente, permitiendo a atacantes identificar vulnerabilidades específicas de esa versión.
[MEDIUM] Puerto 22 (SSH): El puerto de administración remota está abierto, aumentando la superficie de ataque frente a intentos de intrusión por consola.
[MEDIUM] Contenido Mixto: Se detectaron recursos cargados vía HTTP dentro del sitio HTTPS, lo que puede comprometer la integridad de la navegación.
[MEDIUM] Archivo /readme.html: Este archivo de instalación es accesible y revela detalles técnicos del gestor de contenidos que deberían ser privados.
[LOW] Server header expuesto: El servidor responde con la cabecera LiteSpeed, revelando la tecnología subyacente y facilitando el perfilado del sistema.
[LOW] Meta generator: La presencia de etiquetas de Elementor expone versiones de complementos y configuraciones internas del diseño web.
[LOW] Ruta sensible en robots.txt: El archivo de indexación menciona directorios administrativos, lo que guía a posibles atacantes hacia rutas de gestión.