EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://reneproduce.com	Checks	9 pruebas
Dominio	reneproduce.com	Hallazgos	49 totales
Fecha	20 de abril de 2026 a las 22:19	Problemas	16 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha resultado en una puntuación de 60/100, lo que otorga una calificación de grado C. Durante la evaluación se ejecutaron 9 comprobaciones pasivas, obteniendo 5 resultados satisfactorios, 1 advertencia y 3 fallos críticos en la configuración. El sitio presenta debilidades importantes en la protección de datos y en la exposición de información técnica sensible del servidor. Se concluye que el sitio es actualmente vulnerable ante ataques de inyección, suplantación y explotación de vulnerabilidades conocidas en su gestor de contenidos.

Resumen de Riesgos

0	5	9	2	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 321 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
Version CMS Expuesta	20	FALLO	WordPress 6.1.10 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	4 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 321 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  321 dias restantes (expira: 2027-03-07T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-04T00:00:00.000Z
- 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: Apache — 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://www.reneproduce.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

- 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
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.1.10 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.1.10 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 — 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

4 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://fonts.googleapis.com/css?family=Karla:400,700,700ital...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.facebook.com/pages/RENE-PRODUCE/130161247017250
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.twitter.com/reneproduce
- MEDIO **href (link/stylesheet)**
  ...y 1 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (120 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://www.reneproduce.com/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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: La versión 6.1.10 está expuesta públicamente, permitiendo a posibles atacantes identificar y explotar CVEs conocidos.
[HIGH] Content-Security-Policy: Falta esta cabecera, la cual es vital para prevenir ataques de Cross-Site Scripting (XSS) e inyección de contenido.
[HIGH] X-Frame-Options: La ausencia de esta cabecera hace que el sitio sea susceptible a ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide que el navegador fuerce siempre conexiones seguras a través de HTTPS.
[HIGH] HSTS (Strict-Transport-Security): El mecanismo de seguridad no está activo, dejando la conexión vulnerable a ataques de degradación de protocolo.
[MEDIUM] Contenido Mixto: Se detectaron 4 recursos (fuentes de Google y enlaces a redes sociales) que cargan mediante HTTP en una página HTTPS, comprometiendo la integridad de la sesión.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es accesible de forma pública, facilitando ataques de fuerza bruta.
[MEDIUM] Archivo /readme.html: Este archivo es accesible y puede revelar detalles específicos sobre la instalación y versión del CMS.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que podría derivar en la ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy: No existe una política definida para controlar cuánta información de navegación se envía a otros sitios.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la geolocalización.
[LOW] Server header expuesto: La cabecera revela que se utiliza el servidor Apache, facilitando el reconocimiento del entorno técnico.
[LOW] Ruta sensible en robots.txt: La referencia directa a directorios de administración ayuda a los atacantes a mapear áreas restringidas.