EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://rpconsultores.com	Checks	9 pruebas
Dominio	rpconsultores.com	Hallazgos	46 totales
Fecha	18 de agosto de 2026 a las 06:41	Problemas	17 detectados

D

49/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio rpconsultores.com ha arrojado una puntuación de 49/100, lo que corresponde a una calificación de grado D. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 1 generó una advertencia y 4 fueron fallos críticos. Se han detectado deficiencias importantes en la configuración del servidor y en la implementación de protocolos de transporte seguro. Debido a la ausencia de cabeceras de protección y puertos inseguros abiertos, se concluye que el sitio es actualmente vulnerable a diversos vectores de ataque.

Resumen de Riesgos

0	6	9	2	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 57 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	6 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 57 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  57 dias restantes (expira: 2026-10-14T06:53:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-16T06:54:00.000Z
- 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

- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- 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 — 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 (src (script/img/iframe))**
  http://platform.twitter.com/widgets/hub.1326407570.html
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://platform.twitter.com/widgets/hub.1326407570.html
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://fonts.googleapis.com/css?family=Play:400,700
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.netsolution.pe
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.netsolution.pe
- MEDIO **href (link/stylesheet)**
  ...y 1 mas del mismo tipo

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 — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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] Falta de Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques XSS y la inyección de contenido no autorizado.
[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking al permitir que sea cargado dentro de frames externos.
[HIGH] Falta de Strict-Transport-Security: No se obliga al navegador a usar HTTPS, permitiendo ataques de degradación de protocolo.
[HIGH] Ausencia de redirección HTTP a HTTPS: El servidor no fuerza el cifrado, permitiendo que los usuarios naveguen por canales inseguros.
[HIGH] Puerto 21 (FTP) abierto: Este puerto permite la transferencia de archivos sin cifrar, lo que expone credenciales y datos a intercepciones.
[MEDIUM] Falta de X-Content-Type-Options: Permite que el navegador realice MIME-sniffing, aumentando el riesgo de ejecución de archivos maliciosos.
[MEDIUM] Falta de Referrer-Policy: No se controla la información de referencia enviada a otros sitios, lo que puede filtrar URLs privadas.
[MEDIUM] Falta de Permissions-Policy: No existen restricciones sobre el uso de APIs sensibles como la cámara o el micrófono del usuario.
[MEDIUM] Presencia de contenido mixto: Se han detectado 6 recursos (scripts y estilos) cargando por HTTP dentro de la sesión segura HTTPS.
[LOW] Ausencia de archivos robots.txt y sitemap.xml: La falta de estos archivos dificulta la auditoría de rutas y la indexación correcta del sitio.