EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.rsonet.com.ar/	Checks	9 pruebas
Dominio	www.rsonet.com.ar	Hallazgos	48 totales
Fecha	16 de julio de 2026 a las 01:30	Problemas	14 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado ha otorgado una puntuación de 68/100, resultando en una calificación de grado C. Se ejecutaron un total de 9 checks pasivos, obteniendo 6 resultados satisfactorios, 1 advertencia y 2 fallos críticos en la configuración. Aunque el cifrado de datos es correcto, la ausencia total de cabeceras de seguridad y la exposición de versiones de software comprometen la integridad del servidor. Debido a estas omisiones técnicas, se concluye que el sitio es actualmente vulnerable a ataques de inyección y suplantación de identidad. El riesgo detectado es moderado-alto y requiere intervención inmediata para corregir deficiencias estructurales.

Resumen de Riesgos

0	5	5	4	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 56 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, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 7.0.1 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 56 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  56 dias restantes (expira: 2026-09-10T13:12:18.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-12T13:12:19.000Z
- 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: Microsoft-IIS/8.5 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.4.11, ASP.NET — Revela framework/lenguaje
- 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.rsonet.com.ar/
- 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, 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: WordPress 7.0.1
- INFO **Tecnologias detectadas**
  PHP/8.4.11, ASP.NET

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0.1 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0.1 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 — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (118 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.rsonet.com.ar/wp-sitemap.xml
- 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] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de inyección de código y XSS.
[HIGH] X-Frame-Options: La ausencia de esta directiva permite ataques de clickjacking al no restringir cómo se muestra el sitio en marcos externos.
[HIGH] Strict-Transport-Security: No se fuerza el protocolo HTTPS mediante HSTS, permitiendo posibles degradaciones de conexión.
[HIGH] Exposición de versión de WordPress: La versión 7.0.1 es visible públicamente, facilitando que atacantes busquen vulnerabilidades específicas para dicho software.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación que se envía a otros sitios web al seguir enlaces.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, dejando expuestas funciones como la cámara o el micrófono a posibles abusos.
[MEDIUM] Archivo /readme.html expuesto: Este archivo es accesible y revela detalles técnicos innecesarios sobre la instalación del CMS.
[MEDIUM] Panel de login expuesto: La ruta /wp-login.php está disponible para cualquier usuario, aumentando el riesgo de ataques de fuerza bruta.
[LOW] Server header expuesto: El servidor revela el uso de Microsoft-IIS/8.5, proporcionando información valiosa para una fase de reconocimiento.
[LOW] X-Powered-By expuesto: Se detectó el uso de PHP/8.4.11 y ASP.NET, lo que ayuda a identificar vectores de ataque específicos.
[LOW] Meta generator: La etiqueta meta expone explícitamente el uso de WordPress, facilitando el perfilado del sitio.
[LOW] Ruta sensible en robots.txt: Se hace referencia al directorio "admin", señalando directamente rutas de gestión a posibles atacantes.