EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://rawson-chubut.com.ar	Checks	9 pruebas
Dominio	rawson-chubut.com.ar	Hallazgos	46 totales
Fecha	18 de abril de 2026 a las 04:28	Problemas	11 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar la auditoria técnica de ciberseguridad, el sitio web presenta una puntuación de 65/100, lo que equivale a una nota de C. Se ejecutaron 9 checks pasivos, obteniendo 5 resultados satisfactorios, 2 advertencias y 2 fallos críticos en la configuración. Aunque el cifrado de datos es correcto, la ausencia de cabeceras de seguridad y la falta de redirección forzada a conexiones seguras debilitan la postura defensiva del servidor. En su estado actual, el sitio se considera vulnerable a ataques de interceptación de tráfico y explotación de vulnerabilidades en el lado del cliente.

Resumen de Riesgos

0	4	4	3	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 88 dias
Cabeceras de Seguridad	30	FALLO	Solo 2/6 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	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 88 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  88 dias restantes (expira: 2026-07-15T13:12:29.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-16T13:12:30.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 30/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Next.js — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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
- INFO **Tecnologias detectadas**
  React, Next.js, Next.js

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 — 100/100

Estado: OK

No se detecto contenido mixto

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

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1738 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- 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): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyecciones de contenido malicioso al no restringir el origen de los recursos.
[HIGH] Strict-Transport-Security: No se detectó la cabecera HSTS, lo que impide que el navegador fuerce automáticamente conexiones HTTPS seguras en futuras visitas.
[HIGH] Redirección HTTP a HTTPS: El sitio permite el acceso mediante el protocolo HTTP sin cifrar, exponiendo los datos de los usuarios a interceptaciones de tipo Man-in-the-Middle.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó un puerto de servicio web alternativo abierto, lo que incrementa la superficie de ataque y puede exponer servicios no destinados al público.
[MEDIUM] Referrer-Policy: La falta de esta política puede provocar la filtración de información sensible sobre la procedencia de los usuarios hacia dominios de terceros.
[MEDIUM] Permissions-Policy: Al no estar configurada, no existen restricciones sobre el acceso de las APIs del navegador a componentes de hardware o funciones del dispositivo del usuario.
[MEDIUM] Bloqueo total en robots.txt: El archivo bloquea la indexación de todo el sitio mediante la directiva Disallow: /, lo que afecta negativamente al posicionamiento y gestión del tráfico.
[LOW] Server header expuesto: El servidor revela que utiliza Cloudflare, proporcionando información técnica valiosa para un atacante durante la fase de reconocimiento.
[LOW] X-Powered-By expuesto: La cabecera revela el uso del framework Next.js, permitiendo a actores maliciosos buscar vulnerabilidades específicas relacionadas con dicha tecnología.
[LOW] sitemap.xml: El archivo no fue encontrado, lo que dificulta la identificación de la estructura legítima del sitio para herramientas de seguridad y motores de búsqueda.