EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://app.ruteo.com.ar	Checks	9 pruebas
Dominio	app.ruteo.com.ar	Hallazgos	44 totales
Fecha	7 de agosto de 2026 a las 01:30	Problemas	12 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el sitio web determinó una puntuación de 59/100, lo que equivale a una calificación de grado D. Durante la auditoría se ejecutaron 9 comprobaciones pasivas, resultando en 5 verificaciones correctas, 2 advertencias por configuraciones subóptimas y 2 fallos críticos en la infraestructura de seguridad. Los resultados indican una ausencia total de cabeceras de protección y fallos en la implementación de protocolos de transporte seguro. Debido a estas deficiencias, el sitio se considera actualmente vulnerable ante ataques de interceptación y manipulación de contenido.

Resumen de Riesgos

0	5	5	2	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 63 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	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 63 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  63 dias restantes (expira: 2026-10-08T23:31:16.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-10T22:32:40.000Z
- 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: cloudflare — 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 — 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 — 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 (1836 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] Falta de redirección HTTPS: El sitio permite conexiones a través de HTTP sin redirigir al usuario a la versión cifrada, dejando los datos expuestos.
[HIGH] Ausencia de HSTS: No se ha configurado la cabecera Strict-Transport-Security, lo que permite ataques de degradación de protocolo (SSL Stripping).

[HIGH] Falta de Content-Security-Policy: La ausencia de CSP facilita la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).
[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking al no restringir si la página puede ser embebida en marcos externos.
[MEDIUM] Puerto 8080 abierto: La exposición del puerto HTTP-Alt representa un vector de ataque adicional al revelar un servidor web alternativo o proxy.
[MEDIUM] Falta de X-Content-Type-Options: Sin esta cabecera, el navegador puede intentar interpretar archivos de forma incorrecta, permitiendo la ejecución de malware.
[MEDIUM] Bloqueo total en robots.txt: El archivo de rastreo bloquea todo el contenido del sitio, lo que puede afectar la visibilidad y el comportamiento de bots legítimos.
[MEDIUM] Falta de Referrer-Policy: No se controla qué información de procedencia se envía a terceros, comprometiendo la privacidad de la navegación.
[MEDIUM] Falta de Permissions-Policy: No existen restricciones sobre el uso de APIs del navegador como la cámara, el micrófono o la ubicación.
[LOW] Cabecera Server expuesta: Se detectó el valor Server: cloudflare, lo cual revela información tecnológica que ayuda a un atacante en su fase de reconocimiento.
[LOW] Falta de sitemap.xml: La ausencia de un mapa del sitio dificulta la correcta indexación y auditoría de la estructura web.