EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://rame.gyro.com.ar/https://rame.gyro.com.ar/	Checks	9 pruebas
Dominio	rame.gyro.com.ar	Hallazgos	45 totales
Fecha	14 de septiembre de 2026 a las 12:21	Problemas	12 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web auditado presenta una puntuación de seguridad de 72/100, lo que le otorga una calificación de grado C. Durante la evaluación se realizaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, se identificó 1 advertencia y 2 fallos críticos en la configuración de cabeceras y archivos de sistema. Aunque el cifrado de datos es correcto, la ausencia total de políticas de seguridad en el servidor deja a los usuarios expuestos a ataques conocidos. La falta de mecanismos de protección activa y la visibilidad de rutas administrativas permiten concluir que el sitio es vulnerable y requiere intervenciones inmediatas.

Resumen de Riesgos

0	4	5	3	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 79 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	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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 79 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  79 dias restantes (expira: 2026-12-02T16:57:24.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-03T16:57:25.000Z
- 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: nginx/1.24.0 (Ubuntu) — 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://rame.gyro.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

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

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)
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente

- 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 — 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 — 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 Inteligencia Artificial

---RESUMEN EJECUTIVO---
El sitio web auditado presenta una puntuación de seguridad de 72/100, lo que le otorga una calificación de grado C. Durante la evaluación se realizaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, se identificó 1 advertencia y 2 fallos críticos en la configuración de cabeceras y archivos de sistema. Aunque el cifrado de datos es correcto, la ausencia total de políticas de seguridad en el servidor deja a los usuarios expuestos a ataques conocidos. La falta de mecanismos de protección activa y la visibilidad de rutas administrativas permiten concluir que el sitio es

vulnerable y requiere intervenciones inmediatas.

---VULNERABILITIES---
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados, facilitando ataques de XSS e inyección de contenido.
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es vulnerable a clickjacking, permitiendo que atacantes carguen la web en marcos invisibles para engañar al usuario.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones HTTPS, dejando la puerta abierta a ataques de degradación de SSL (Man-in-the-Middle).
[MEDIUM] X-Content-Type-Options: El servidor no previene el sniffing de tipos MIME, lo que podría causar que el navegador ejecute archivos maliciosos disfrazados de elementos legítimos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación enviada a terceros, lo que compromete la privacidad de la ruta de los usuarios.
[MEDIUM] Permissions-Policy: La falta de restricciones en las APIs del navegador permite el acceso potencial a funciones sensibles como la cámara o el micrófono sin políticas claras.
[MEDIUM] Rutas administrativas expuestas: Las rutas /administrator/ y /user/login son accesibles desde internet, lo que facilita ataques de fuerza bruta contra el panel de gestión.
[LOW] Server header expuesto: El servidor revela el uso de nginx/1.24.0 (Ubuntu), proporcionando información valiosa a un atacante sobre versiones de software y sistema operativo.
[LOW] Ausencia de robots.txt y sitemap.xml: El servidor responde con errores 404 para estos archivos, lo que afecta negativamente al rastreo y muestra una falta de mantenimiento en la configuración base.