

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://gr-web-stg.dev.gruporamos.com
Dominio gr-web-stg.dev.gruporamos.com
Fecha 14 de abril de 2026 a las 20:24

Checks 9 pruebas
Hallazgos 12 totales
Problemas 0 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web ha arrojado una puntuación exacta de 100/100, lo que le otorga una calificación de Grado A. Durante la evaluación se ejecutaron 9 checks pasivos, resultando 1 de ellos satisfactorio y 0 fallos detectados, lo que indica una superficie de ataque externa limpia. Al no haberse identificado riesgos de seguridad ni advertencias durante el proceso, se concluye que el sitio es seguro bajo los parámetros analizados. Esta auditoría confirma que la infraestructura visible cumple con los estándares de seguridad requeridos para su nivel de exposición.

Resumen de Riesgos



Resumen de Checks

Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar contenido mixto
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

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 — Envío 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

No se detectaron vulnerabilidades durante el escaneo pasivo ni se reportaron hallazgos por parte del PentestAgent. La revisión de puertos abiertos confirmó que no existen servicios expuestos que puedan comprometer la integridad del servidor. Dado que el resultado final es de cero fallos y cero advertencias, no existen CWEs, cabeceras faltantes ni endpoints de API descubiertos que representen un riesgo en este momento.