EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://guard-dev.obenapps.com/#/controls	Checks	9 pruebas
Dominio	guard-dev.obenapps.com	Hallazgos	12 totales
Fecha	31 de agosto de 2026 a las 13:03	Problemas	0 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis técnico de ciberseguridad realizado sobre el activo digital ha resultado en una puntuación de 100/100, otorgando una nota de A. Durante el proceso se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 1 resultó en estado satisfactorio y ninguna detectó fallos o advertencias directas. No se ha llevado a cabo un pentest activo, por lo que la evaluación se basa en la visibilidad externa inmediata de la infraestructura. Considerando los datos obtenidos, el sitio se clasifica como seguro bajo los parámetros de este escaneo específico. No obstante, la existencia de múltiples errores de tiempo de espera en las pruebas sugiere una restricción en la visibilidad total de la configuración.

Resumen de Riesgos

0	0	0	0	12
CRITICO	ALTO	MEDIO	BAJO	INFO

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 — 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 Seguridad

VULNERABILIDADES DETECTADAS

[BAJA] Puertos Abiertos: No se detectaron puertos de servicios críticos expuestos innecesariamente, reduciendo la superficie de ataque externa. Nota: No se identificaron vulnerabilidades adicionales de tipo CWE, cabeceras faltantes o endpoints expuestos debido a que la mayoría de los checks pasivos resultaron en error de tiempo de espera y el pentest activo no fue ejecutado.