EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.geox1.duckdns.org	Checks	9 pruebas
Dominio	www.geox1.duckdns.org	Hallazgos	13 totales
Fecha	13 de abril de 2026 a las 16:20	Problemas	1 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre geox1.duckdns.org ha concluido con una puntuación perfecta de 100/100 y una calificación de nota A. Se han ejecutado un total de 9 checks pasivos, de los cuales 1 resultó totalmente satisfactorio y los 8 restantes no detectaron ninguna advertencia ni fallo de seguridad. No se han encontrado brechas de seguridad ni configuraciones erróneas que comprometan la integridad del sitio en esta fase. En base a los resultados obtenidos, el sitio se considera seguro bajo el alcance de la metodología de auditoría pasiva empleada.

Resumen de Riesgos

0	1	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	1 puerto(s) abierto(s), todos esperados

Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS

Puertos Abiertos — 100/100

Estado: OK

1 puerto(s) abierto(s), todos esperados

- 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)**
  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 han detectado vulnerabilidades durante el escaneo pasivo realizado. El informe confirma la ausencia total de fallos (0) y advertencias (0) en los parámetros analizados. Debido a que el PentestAgent no fue ejecutado, no se han identificado hallazgos adicionales como CWEs, endpoints de API descubiertos, subdominios expuestos o cabeceras faltantes que afecten la puntuación. La infraestructura evaluada no presenta debilidades críticas ni puntos de explotación activos según los datos registrados.