

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.odl.com.co/	Checks	9 pruebas
Dominio	www.odl.com.co	Hallazgos	18 totales
Fecha	16 de julio de 2026 a las 15:38	Problemas	3 detectados

F

37/100

puntos de seguridad



RESUMEN EJECUTIVO

Tras realizar la auditoría de seguridad en el sitio web analizado, se ha obtenido una puntuación de 37/100 con una calificación de F, lo que representa un nivel de protección deficiente. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales solo uno resultó exitoso, identificando fallos críticos en el cifrado y la configuración básica del servidor. La falta de un certificado SSL válido y la ausencia de archivos de indexación fundamentales comprometen la integridad del sitio. No se realizó un pentest activo, pero los resultados pasivos son concluyentes respecto a la debilidad de la infraestructura actual. En su estado presente, el sitio web es considerado vulnerable y no apto para el manejo de información sensible.

Resumen de Riesgos

1	0	0	2	15
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
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
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: FALLO

Certificado SSL no valido

- CRITICO Certificado valido
El certificado SSL NO es valido
- INFO Días hasta expiracion
63 días restantes (expira: 2026-09-17T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-03-03T00:00:00.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO robots.txt
Error al acceder

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 autentificacion 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

[CRITICAL] Certificado SSL no válido: El certificado de seguridad ha fallado las pruebas de validación, lo que impide establecer conexiones cifradas y seguras con los usuarios.

[LOW] Ausencia de robots.txt: No se pudo acceder al archivo de directivas de rastreo, lo que puede provocar que motores de búsqueda indexen directorios no deseados.

[LOW] Ausencia de sitemap.xml: El sitio carece de un mapa de estructura accesible, lo que dificulta la auditoría de contenidos y la navegación estructurada.

[INFO] Error en validación de cabeceras: No se pudieron verificar las protecciones contra ataques de inyección o cross-site scripting debido a errores de respuesta del servidor.