

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://ferreteriaelgreco.es
Dominio ferreteriaelgreco.es
Fecha 2 de julio de 2026 a las 10:18

Checks 9 pruebas
Hallazgos 19 totales
Problemas 5 detectados

F

23/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el activo digital ha resultado en una puntuación crítica de 23/100, lo que equivale a una nota de F. Los resultados de los checks pasivos indican un estado de vulnerabilidad severo, habiendo ejecutado 9 comprobaciones con un saldo de 0 éxitos, 1 advertencia y 2 fallos críticos. La ausencia de un cifrado válido y la exposición de puertos de gestión suponen un riesgo inmediato para la integridad de la plataforma. Se concluye que el sitio es vulnerable y no cumple con los estándares mínimos de seguridad para operar en internet.

Resumen de Riesgos



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	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 0/100

Estado: FALLO

Certificado SSL no valido

- CRITICO** Certificado valido
El certificado SSL NO es valido
- INFO** Dias hasta expiracion
155 dias restantes (expira: 2026-12-03T23:59:59.000Z)
- INFO** Fecha de emision
Emitido desde: 2026-05-19T00:00:00.000Z
- INFO** Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- INFO** HTTP !' HTTPS redireccion
HTTP 301 redirige a https://www.ferreteriaelgreco.es/

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO** robots.txt
Error al acceder
- BAJO** sitemap.xml
Error al acceder

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- ALTO** Puerto 21 (FTP)
ABIERTO — Transferencia de archivos sin cifrar
- MEDIO** Puerto 22 (SSH)
ABIERTO — Acceso remoto seguro
- INFO** Puerto 23 (Telnet)
Cerrado — Acceso remoto sin cifrar
- INFO** Puerto 25 (SMTP)
Cerrado — Envío de correo
- INFO** Puerto 80 (HTTP)
Abierto (esperado) — Servidor web
- INFO** Puerto 443 (HTTPS)
Abierto (esperado) — 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

Análisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICO] Certificado SSL no valido: El sitio no cuenta con cifrado activo, lo que permite la interceptacion de datos sensibles entre el usuario y el servidor.

[ALTO] Puerto 21 (FTP) abierto: El servicio de transferencia de archivos esta expuesto y utiliza protocolos sin cifrar, facilitando el robo de credenciales de administracion.

[MEDIO] Puerto 22 (SSH) abierto: La visibilidad publica de este puerto permite ataques de fuerza bruta para intentar tomar el control total del servidor.

[BAJO] Ausencia de robots.txt: No existe una configuracion para guiar a los rastreadores, lo que puede exponer rutas sensibles a los motores de busqueda.

[BAJO] Ausencia de sitemap.xml: La falta de este archivo impide una auditoria adecuada de la estructura del sitio y dificulta su indexacion controlada.

[ALTO] Fallo en cabeceras de seguridad: La imposibilidad de verificar las cabeceras indica que el sitio carece de protecciones basicas contra ataques de inyeccion y suplantacion.