EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.comercialudra.es	Checks	9 pruebas
Dominio	www.comercialudra.es	Hallazgos	47 totales
Fecha	9 de abril de 2026 a las 15:47	Problemas	16 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio comercialudra.es ha otorgado una puntuación de 62/100, lo que equivale a una nota C. Durante la auditoría se ejecutaron 9 checks pasivos, resultando en 4 verificaciones superadas, 3 advertencias y 2 fallos críticos. Se han identificado riesgos significativos relacionados con la exposición de bases de datos y la falta de cabeceras de protección esenciales. Debido a la presencia de puertos críticos abiertos y una versión de CMS desactualizada, el sitio se clasifica actualmente como vulnerable. Es imperativo aplicar las correcciones técnicas detalladas para mitigar posibles ataques externos.

Resumen de Riesgos

1	6	4	5	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 249 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 6.9.4 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 249 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  249 dias restantes (expira: 2026-12-14T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-11-13T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PleskLin — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.comercialudra.es/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  Next.js, PleskLin

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.9.4 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- INFO **Archivo /README.txt**
  No accesible (correcto)

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (35 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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)**
  Abierto (esperado) — Servidor web seguro
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL): ABIERTO — La base de datos está expuesta a internet, lo que permite ataques de fuerza bruta o explotación directa de datos sensibles.
[HIGH] Puerto 21 (FTP): ABIERTO — Protocolo de transferencia de archivos sin cifrar que permite la interceptación de credenciales y datos en tránsito.
[HIGH] WordPress version: Versión 6.9.4 expuesta — El uso de una versión antigua permite a atacantes explotar vulnerabilidades conocidas (CVEs) ya corregidas en versiones modernas.
[HIGH] Content-Security-Policy: Falta — La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: Falta — El sitio es vulnerable a ataques de clickjacking, permitiendo que terceros carguen la web en marcos invisibles para engañar al usuario.
[HIGH] Strict-Transport-Security: Falta — No se obliga al navegador a usar conexiones HTTPS (HSTS), permitiendo ataques de degradación de SSL.
[MEDIUM] X-Content-Type-Options: Falta — Permite el MIME-type sniffing, lo que puede llevar a la ejecución de archivos no ejecutables como scripts.
[MEDIUM] Referrer-Policy: Falta — No se controla la información de procedencia enviada en las peticiones, lo que puede filtrar URLs internas.
[MEDIUM] Permissions-Policy: Falta — El sitio no restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la ubicación.
[MEDIUM] Archivo /readme.html: Accesible — Este archivo público revela detalles técnicos sobre la instalación y versión del CMS WordPress.
[LOW] Server header expuesto: Apache — Revela la tecnología y versión del servidor web, facilitando la búsqueda de vulnerabilidades específicas de la infraestructura.
[LOW] X-Powered-By expuesto: PleskLin — Informa sobre el panel de control y sistema operativo subyacente, reduciendo el esfuerzo de reconocimiento para un atacante.
[LOW] Meta generator: WordPress 6.9.4 — Expone directamente la versión del software en el código fuente de la página.
[LOW] Ruta sensible en robots.txt: Referencia a "admin" — Indica a los rastreadores y atacantes la ubicación de directorios administrativos o rutas privadas.
[LOW] sitemap.xml: No encontrado — La ausencia de este archivo dificulta la auditoría de la estructura del sitio y afecta negativamente al SEO técnico.