EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.elingenio.es/	Checks	9 pruebas
Dominio	www.elingenio.es	Hallazgos	47 totales
Fecha	25 de mayo de 2026 a las 11:24	Problemas	10 detectados

B

75/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 75/100 con una calificación de B. Se han ejecutado 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias y 1 fue calificado como fallo crítico. Los resultados indican que, aunque el cifrado de transporte es correcto, existen deficiencias graves en la configuración del servidor y la exposición de servicios internos. El diagnóstico concluye que el sitio es vulnerable debido a la visibilidad pública de puertos críticos y versiones de software específicas. Se requiere una intervención inmediata para mitigar riesgos de intrusión y exfiltración de datos.

Resumen de Riesgos

1	5	1	3	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 45 dias
Cabeceras de Seguridad	55	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 1779697442 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 45 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  45 dias restantes (expira: 2026-07-09T17:31:51.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-10T17:31:52.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.2.31 — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(self), microphone=(), camera=()

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.elingenio.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, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WPML ver:4.9.4 stt:1,2;
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.2.31

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 1779697442 expuesta

- ALTO **WordPress version**
  Version 1779697442 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)

- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (51 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 0 Allow
- INFO **sitemap.xml**
  Presente, ? URLs
- 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): La base de datos está abierta a conexiones externas, lo que permite intentos de acceso no autorizados y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP): El servicio de transferencia de archivos está expuesto y opera sin cifrado, permitiendo la interceptación de credenciales.
[HIGH] WordPress version: La versión específica del sistema (1779697442) es pública, facilitando que atacantes identifiquen vulnerabilidades conocidas.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite ataques de scripts cruzados (XSS) e inyección de contenido malicioso.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el sitio obligue a los navegadores a usar siempre conexiones cifradas.
[MEDIUM] Ruta /wp-login.php: El panel de administración de WordPress es accesible públicamente, aumentando el riesgo de ataques automatizados de login.
[LOW] Server header expuesto: El servidor LiteSpeed revela su identidad técnica, proporcionando información útil para la fase de reconocimiento de un ataque.
[LOW] X-Powered-By expuesto: La cabecera revela el uso de PHP/8.2.31, permitiendo a los atacantes dirigir exploits específicos para esa versión.
[LOW] Meta generator: La etiqueta meta expone detalles del plugin WPML y su versión, ampliando la superficie de ataque informada.