EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://eltallerdealex.com/#	Checks	9 pruebas
Dominio	eltallerdealex.com	Hallazgos	44 totales
Fecha	18 de mayo de 2026 a las 12:18	Problemas	13 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja una puntuación técnica de 60/100, lo que resulta en una calificación de nota C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron correctos, se detectó 1 advertencia y se identificaron 3 fallos críticos de seguridad. A pesar de contar con un cifrado de conexión válido, la exposición de servicios críticos de bases de datos y la ausencia total de cabeceras de protección elevan el riesgo de compromiso. Se concluye que el sitio es vulnerable y requiere medidas correctivas inmediatas para proteger la integridad de su infraestructura.

Resumen de Riesgos

2	5	4	2	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 87 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 2 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	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 87 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  87 dias restantes (expira: 2026-08-13T05:11:41.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-15T05:11:42.000Z
- 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: nginx — Revela tecnologia del servidor

- 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://eltallerdealex.com/
- 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
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 2 expuesta

- 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (116 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://eltallerdealex.com/sitemaps.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- 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
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — 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): Base de datos MySQL abierta y expuesta a internet, lo que permite ataques de fuerza bruta y acceso no autorizado.
[CRITICAL] Puerto 5432 (PostgreSQL): Base de datos PostgreSQL accesible públicamente, facilitando la posible exfiltración de información sensible.
[HIGH] Puerto 21 (FTP): El servicio de transferencia de archivos está abierto y opera sin cifrado, permitiendo la interceptación de credenciales en texto plano.

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Falta de protección contra ataques de clickjacking, lo que permite a terceros cargar el sitio en marcos invisibles.
[HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, dejando a los usuarios vulnerables a ataques de degradación de conexión.
[MEDIUM] Versión de WordPress expuesta: El archivo readme.html es accesible y puede revelar información técnica específica del CMS a atacantes.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido, facilitando ataques de ejecución de scripts.
[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación que se envía a otros sitios web mediante el referente.
[MEDIUM] Permissions-Policy: Ausencia de restricciones sobre el acceso de las APIs del navegador a funciones sensibles como cámara o micrófono.
[LOW] Cabecera de servidor expuesta: El servidor revela el uso de nginx, lo que ayuda a los atacantes a buscar vulnerabilidades específicas para esa tecnología.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a directorios de administración, lo que ayuda a los atacantes a mapear áreas sensibles del sitio.