EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.elmayoristadeltextil.es	Checks	9 pruebas
Dominio	www.elmayoristadeltextil.es	Hallazgos	48 totales
Fecha	6 de mayo de 2026 a las 13:14	Problemas	13 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada a elmayoristadeltextil.es arroja una puntuación de 64/100, lo que equivale a una nota C. El análisis se basó en la ejecución de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, uno presentó advertencias y tres fallaron con hallazgos de severidad alta. Se han identificado deficiencias críticas en la configuración de cabeceras de seguridad y una exposición peligrosa de servicios de infraestructura como la base de datos. Debido a la falta de protecciones básicas contra ataques de interceptación y la visibilidad de puertos administrativos, el sitio se considera actualmente vulnerable. Es imperativo abordar los hallazgos técnicos para mitigar riesgos de intrusión y compromiso de datos de terceros.

Resumen de Riesgos

1	5	5	2	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 61 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 61 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  61 dias restantes (expira: 2026-07-06T03:05:10.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-07T03:05:11.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.30, 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
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.elmayoristadeltextil.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- 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, PHP/8.3.30, PleskLin

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)

- INFO **Archivo /README.txt**
  No accesible (correcto)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 robots.txt

- INFO **sitemap.xml**
  Presente, 81 URLs
- 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
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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 es accesible desde internet, permitiendo ataques de fuerza bruta o explotación directa.
[HIGH] Puerto 21 (FTP) abierto: El uso de este protocolo transfiere datos y credenciales sin cifrado, facilitando la interceptación de información.
[HIGH] Falta de Content-Security-Policy: La ausencia de esta directiva permite la ejecución de scripts maliciosos mediante ataques XSS.
[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a clickjacking al permitir que el contenido sea cargado en marcos externos no autorizados.
[HIGH] Cookie PHPSESSID sin flag HttpOnly: Permite que atacantes accedan a la sesión del usuario a través de scripts en el navegador.
[HIGH] Cookie PHPSESSID sin flag Secure: La información de sesión puede ser enviada por canales no cifrados, comprometiendo la cuenta del usuario.
[MEDIUM] Puerto 22 (SSH) abierto: Un servicio de administración remota expuesto aumenta la superficie de ataque para accesos no autorizados.
[MEDIUM] Falta de X-Content-Type-Options: El sitio no previene el sniffing de tipos MIME, lo que puede llevar a la ejecución involuntaria de archivos maliciosos.
[MEDIUM] Falta de Referrer-Policy: No se controla la información de procedencia enviada a otros dominios, lo que puede filtrar URLs privadas.
[MEDIUM] Falta de Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente el acceso a funciones sensibles del cliente.
[MEDIUM] Cookie PHPSESSID sin flag SameSite: Esta carencia hace que la sesión sea susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[LOW] Falta de archivo robots.txt: No existen instrucciones para rastreadores, lo que dificulta el control de la indexación de directorios.
[LOW] Server header expuesto: El servidor revela que utiliza nginx, facilitando la búsqueda de exploits específicos para ese software.
[LOW] X-Powered-By expuesto: Se divulga el uso de PHP/8.3.30 y Plesk, aportando detalles técnicos valiosos para un atacante.