EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://corporacionfernandezduarez.desarrolladorhansluyo.com/	Checks	9 pruebas
Dominio	corporacionfernandezduarez.desarrolladorhansluyo.com	Hallazgos	49 totales
Fecha	7 de agosto de 2026 a las 04:24	Problemas	13 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 57/100, lo que corresponde a una calificación de grado D. El análisis consistió en 9 checks pasivos, resultando en 4 verificaciones exitosas, 3 advertencias y 2 fallos críticos en la configuración del servidor. Se han detectado debilidades significativas en la protección de datos y la exposición de servicios internos. Debido a la falta de cabeceras de seguridad y la apertura de puertos críticos de bases de datos, se concluye que el sitio es actualmente vulnerable a ataques externos.

Resumen de Riesgos

1	7	3	2	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 31 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	83	AVISO	XSRF-TOKEN: falta HttpOnly
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 31 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  31 dias restantes (expira: 2026-09-07T15:49:07.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-09T15:49:08.000Z
- 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: LiteSpeed — 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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

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

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 — 83/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: textileria_administrador_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: textileria_administrador_session — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: textileria_administrador_session — SameSite**
  SameSite=lax

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 (24 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- 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 directamente a internet, lo que permite intentos de conexión y ataques de fuerza bruta externos.
[HIGH] Puerto 21 (FTP) abierto: Este servicio permite la transferencia de archivos sin cifrado, exponiendo credenciales y datos a interceptaciones.
[HIGH] Falta de redirección HTTPS: El servidor no fuerza el uso de conexiones seguras, permitiendo que la comunicación viaje en texto plano vía HTTP.
[HIGH] Ausencia de Content-Security-Policy: No existe una política para prevenir ataques de inyección de código y Cross-Site Scripting (XSS).
[HIGH] Falta de X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea cargado en frames, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security (HSTS) no configurado: El navegador no es instruido para usar exclusivamente el protocolo seguro HTTPS.
[HIGH] Cookie XSRF-TOKEN sin atributo HttpOnly: El token de seguridad es accesible mediante scripts del navegador, aumentando el riesgo de robo de sesión.
[MEDIUM] X-Content-Type-Options faltante: El sitio es vulnerable a ataques de sniffing de tipos MIME por parte del navegador.
[MEDIUM] Referrer-Policy no definida: Se podría estar filtrando información sensible sobre la procedencia de los usuarios hacia sitios externos.
[MEDIUM] Permissions-Policy ausente: No se restringe el uso de APIs del navegador como la cámara, el micrófono o la ubicación.
[LOW] Cabecera Server expuesta: Se revela el uso del servidor LiteSpeed, lo que ayuda a un atacante a buscar vulnerabilidades específicas para esa tecnología.
[LOW] Archivo sitemap.xml no encontrado: La falta de este archivo dificulta la auditoría de la estructura completa del sitio y su indexación.