EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://salon.tania.fonbec.dedyn.io/	Checks	9 pruebas
Dominio	salon.tania.fonbec.dedyn.io	Hallazgos	45 totales
Fecha	13 de mayo de 2026 a las 20:29	Problemas	14 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio salon.tania.fonbec.dedyn.io arroja una puntuación técnica de 72/100, lo que equivale a una nota de C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 6 verificaciones exitosas, una advertencia y dos fallos críticos en la configuración de seguridad. Aunque el cifrado de datos es correcto, la ausencia total de cabeceras de protección expone la plataforma a diversos vectores de ataque. Por lo tanto, se concluye que el sitio es vulnerable y requiere ajustes inmediatos en su servidor web para alcanzar un nivel de seguridad óptimo.

Resumen de Riesgos

0	4	8	2	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 52 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 52 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  52 dias restantes (expira: 2026-07-04T22:45:37.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-05T22:45:38.000Z
- 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: openresty — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Express — 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://salon.tania.fonbec.dedyn.io/
- 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
- INFO **Tecnologias detectadas**
  Express

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- INFO **Puerto 21 (FTP)**
  Cerrado — 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
- INFO **Puerto 3306 (MySQL)**
  Cerrado — 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

[ALTA] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.

[ALTA] X-Frame-Options: No hay protección configurada contra clickjacking, lo que permite que el sitio sea cargado en frames externos para engañar a usuarios.
[ALTA] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce siempre conexiones cifradas, facilitando ataques de degradación de SSL.
[ALTA] HSTS no configurado: El servidor realiza la redirección a HTTPS pero no instruye al navegador para mantener dicha conexión de forma permanente.
[MEDIA] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que podría llevar al navegador a ejecutar archivos con contenido malicioso.
[MEDIA] Referrer-Policy: No se controla la información de navegación que se envía a otros sitios, lo que puede comprometer la privacidad de las rutas internas.
[MEDIA] Permissions-Policy: No se restringen las APIs del navegador, dejando activos por defecto permisos sensibles como cámara o micrófono.
[MEDIA] Archivos informativos expuestos: Los archivos /readme.html y /README.txt son accesibles y pueden filtrar detalles técnicos sobre la construcción del sitio.
[MEDIA] Paneles de login expuestos: Las rutas /wp-login.php, /administrator/ y /user/login son accesibles públicamente, facilitando ataques de fuerza bruta.
[BAJA] Server header expuesto: El servidor revela el uso de openresty, proporcionando información útil a atacantes para buscar exploits específicos.
[BAJA] X-Powered-By expuesto: Se revela el uso del framework Express, lo que ayuda a identificar la infraestructura y lenguaje de programación utilizado.
[BAJA] Ausencia de Robots.txt y Sitemap: La falta de estos archivos dificulta la gestión correcta del rastreo por parte de buscadores y la organización del contenido.