EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.daviviendaintl.com/#/personas	Checks	9 pruebas
Dominio	www.daviviendaintl.com	Hallazgos	46 totales
Fecha	11 de junio de 2026 a las 04:21	Problemas	9 detectados

B

81/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar el analisis de seguridad en el sitio web, se ha obtenido una puntuacion de 81/100 con una nota final de B. El escaneo consistio exclusivamente en 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 presento fallos criticos de configuracion. Debido a la ausencia de un pentest activo, no se han evaluado vulnerabilidades de ejecucion o logica de negocio. El sitio web se considera parcialmente seguro, presentando una base solida en cifrado pero deficiencias notables en politicas de seguridad del lado del cliente que deben ser subsanadas para mitigar riesgos de inyeccion.

Resumen de Riesgos

0	2	5	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 52 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

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: 2026-08-01T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-07-02T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — 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
- INFO **Strict-Transport-Security**
  Presente: max-age=7776000; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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.daviviendaintl.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=7776000; preload
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- MEDIO **HSTS max-age**
  max-age=7776000 (90 dias) — Recomendado minimo 180 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

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 — 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1738 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: Falta — La ausencia de esta cabecera permite la ejecucion de scripts no autorizados, aumentando el riesgo de ataques XSS y de inyeccion de contenido malicioso.
[HIGH] X-Frame-Options: Falta — Sin esta directiva, el sitio es vulnerable a ataques de clickjacking, donde un atacante puede cargar la web en un marco invisible para engañar al usuario.
[MEDIUM] Puerto 8080 (HTTP-Alt): ABIERTO — La presencia de un servidor web alternativo o proxy en este puerto aumenta la superficie de ataque y podria exponer servicios internos no deseados.
[MEDIUM] Referrer-Policy: Falta — No se controla que informacion de referencia se envia a otros dominios, lo que podria comprometer la privacidad de la navegacion del usuario.
[MEDIUM] Permissions-Policy: Falta — No se restringen las APIs del navegador, permitiendo potencialmente que scripts accedan a funciones como la camara o el microfono si existiera otra vulnerabilidad.
[MEDIUM] HSTS max-age: Configuracion corta — El valor actual es de 90 dias, mientras que el estandar de la industria recomienda un minimo de 180 dias para garantizar una conexion segura persistente.
[MEDIUM] robots.txt: Bloqueo total — El archivo prohibe el rastreo de todo el sitio, lo cual es inusual y podria ocultar problemas de acceso o configuraciones erroneas de indexacion.
[LOW] Server header expuesto: Server: cloudflare — El servidor revela la tecnologia de infraestructura utilizada, lo que ayuda a posibles atacantes en la fase de reconocimiento.
[LOW] sitemap.xml: No encontrado — La falta de este archivo dificulta la auditoria completa de la estructura del sitio y afecta la transparencia del mapa web.