EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Www.familiaverde.mx	Checks	9 pruebas
Dominio	www.familiaverde.mx	Hallazgos	51 totales
Fecha	6 de agosto de 2026 a las 07:02	Problemas	9 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio familiaverde.mx ha arrojado una puntuación de 72/100, lo que resulta en una calificación de grado C. Durante la auditoría se realizaron 9 checks pasivos, de los cuales 5 fueron satisfactorios, 3 generaron advertencias y 1 falló por completo debido a configuraciones críticas ausentes. Si bien el sitio posee un cifrado de transporte robusto, carece de todas las cabeceras de seguridad modernas y presenta deficiencias en la gestión de cookies. En su estado actual, el sitio se considera vulnerable a ataques de inyección, clickjacking y secuestro de sesiones.

Resumen de Riesgos

0	5	3	1	42
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 64 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	89	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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 64 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  64 dias restantes (expira: 2026-10-08T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-09-09T00:00:00.000Z
- 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

- 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://www.familiaverde.mx/
- 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 — 89/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO **Cookies detectadas**
  3 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: laravel_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: laravel_session — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: laravel_session — SameSite**
  SameSite=lax
- INFO **Cookie: 5VRerEYkbIVzZLhfmvN0wwymyw9UjJHEFgLx6o0S — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: 5VRerEYkbIVzZLhfmvN0wwymyw9UjJHEFgLx6o0S — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: 5VRerEYkbIVzZLhfmvN0wwymyw9UjJHEFgLx6o0S — 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 — 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 está configurada, lo que permite que el sitio sea cargado en iframes ajenos, facilitando ataques de clickjacking.
[ALTA] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras, permitiendo ataques de degradación de protocolo (SSL Stripping).
[ALTA] Cookie XSRF-TOKEN: Falta el atributo HttpOnly, lo cual permite que la cookie de seguridad sea accesible mediante JavaScript, elevando el riesgo de robo de identidad.
[MEDIA] X-Content-Type-Options: Al no estar presente, el navegador puede intentar interpretar archivos con formatos incorrectos, abriendo la puerta a ejecución de código malicioso.
[MEDIA] Referrer-Policy: No se controla la información de referencia enviada a sitios externos, lo que podría exponer rutas privadas de la aplicación.
[MEDIA] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como cámara, micrófono o geolocalización.
[BAJA] sitemap.xml: El archivo de mapa de sitio no fue encontrado, lo que dificulta la indexación y visibilidad de la estructura web.