EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://variedadeskarendaniela.com/	Checks	9 pruebas
Dominio	variedadeskarendaniela.com	Hallazgos	47 totales
Fecha	12 de julio de 2026 a las 16:37	Problemas	11 detectados

C

67/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al dominio variedadeskarendaniela.com arroja una puntuación de 67/100, lo que resulta en una nota de C. Durante el análisis se ejecutaron un total de 9 checks pasivos, de los cuales 3 resultaron satisfactorios, 4 generaron advertencias y 1 fue identificado como fallo crítico. Se han detectado deficiencias importantes en la configuración de las cabeceras de seguridad y en el manejo de las cookies de sesión, que carecen de atributos esenciales de protección. Debido a la falta de mecanismos para forzar conexiones seguras y prevenir ataques de inyección, el sitio se considera vulnerable ante posibles interceptaciones de datos y ataques de scripts entre sitios.

Resumen de Riesgos

0	6	3	2	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 59 dias
Cabeceras de Seguridad	30	FALLO	Solo 2/6 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
Seguridad de Cookies	50	AVISO	XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Se...
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): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 59 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  59 dias restantes (expira: 2026-09-09T21:15:16.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-11T21:15:17.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 30/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx/1.18.0 (Ubuntu) — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://variedadeskarendaniela.com/
- 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**
  Next.js

Seguridad de Cookies — 50/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Secure; variedadeskd_session: falta Secure

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: XSRF-TOKEN — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax

- INFO **Cookie: variedadeskd_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: variedadeskd_session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: variedadeskd_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

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

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

[HIGH] Content-Security-Policy (CSP): Falta esta cabecera fundamental que previene ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso.

[HIGH] Strict-Transport-Security (HSTS): No está configurada la instrucción que obliga al navegador a comunicarse exclusivamente mediante HTTPS, permitiendo ataques de degradación de protocolo.
[HIGH] Cookie XSRF-TOKEN: Carece de los atributos HttpOnly y Secure, lo que permite que el token sea accesible mediante scripts del lado del cliente y se envíe por canales no cifrados.
[HIGH] Cookie variedadeskd_session: No tiene activo el flag Secure, permitiendo que la cookie de sesión viaje a través de conexiones HTTP inseguras.
[MEDIUM] Referrer-Policy: La ausencia de esta política impide controlar qué información de navegación se comparte con otros sitios web al seguir enlaces.
[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de APIs del navegador, como el acceso a la ubicación, cámara o micrófono.
[MEDIUM] Puerto 22 (SSH) abierto: Se detectó el puerto de administración remota expuesto a internet, lo cual es un vector común para ataques de fuerza bruta.
[LOW] Cabecera de servidor expuesta: El campo Server revela el uso de nginx/1.18.0 (Ubuntu), proporcionando información técnica valiosa para un atacante.
[LOW] Ausencia de sitemap.xml: No se encontró el archivo de mapa del sitio, lo que representa una falta de optimización técnica y estructural.