EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://juanadecohome.com.ar/	Checks	9 pruebas
Dominio	juanadecohome.com.ar	Hallazgos	48 totales
Fecha	14 de julio de 2026 a las 20:06	Problemas	14 detectados

C

69/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha arrojado una puntuación de 69/100, lo que equivale a una nota de C. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron calificados como fallos críticos. Al no haberse realizado un pentest activo, los resultados se limitan a la superficie de exposición pública y configuraciones de red visibles. En su estado actual, el sitio se considera vulnerable debido a la exposición de información sensible y la ausencia de protecciones básicas contra ataques comunes.

Resumen de Riesgos

0	4	6	4	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 49 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 7.0.1 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 49 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  49 dias restantes (expira: 2026-09-01T20:31:31.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-03T20:31:32.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: hcdn — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.30 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- 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://juanadecohome.com.ar/
- 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

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 7.0.1
- INFO **Tecnologias detectadas**
  React, Next.js, PHP/8.3.30

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0.1 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0.1 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://google.com/maps?ll=-33.120872,-64.359024&z=16&#0...

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (323 bytes)
- INFO **Reglas robots.txt**
  6 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://juanadecohome.com.ar/wp-sitemap.xml
- 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

[HIGH] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea embebido en frames externos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide que el navegador fuerce conexiones seguras y permite ataques de degradación de SSL.
[HIGH] WordPress version: La versión 7.0.1 se encuentra expuesta públicamente, permitiendo a potenciales atacantes identificar vulnerabilidades específicas para esta versión.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que los navegadores realicen sniffing de tipos MIME, lo que podría derivar en la ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy: No existe una política definida, lo que puede provocar la fuga de información sensible en las cabeceras de referencia hacia otros dominios.
[MEDIUM] Permissions-Policy: La falta de restricciones permite que el sitio acceda potencialmente a APIs del navegador como cámara o micrófono sin una política de seguridad estricta.
[MEDIUM] Contenido Mixto: Se detectó un recurso stylesheet cargado mediante HTTP (Google Maps), lo que debilita la integridad de la conexión cifrada.
[MEDIUM] Archivo readme.html: Este archivo es accesible públicamente y suele revelar información técnica detallada sobre la instalación del CMS.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es visible para cualquier usuario, quedando expuesto a ataques de fuerza bruta.
[LOW] Cabecera Server expuesta: Se revela el uso de la tecnología hcdn, facilitando el reconocimiento del entorno del servidor.
[LOW] Cabecera X-Powered-By expuesta: Se muestra el uso de PHP/8.3.30, lo que permite acotar la búsqueda de exploits para dicha versión del lenguaje.
[LOW] Meta generator: El código fuente expone explícitamente el uso de WordPress 7.0.1.
[LOW] Rutas sensibles en robots.txt: Se hace referencia directa a directorios de administración, orientando a los atacantes sobre la estructura interna del sitio.