EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.wix.com	Checks	9 pruebas
Dominio	www.wix.com	Hallazgos	57 totales
Fecha	5 de mayo de 2026 a las 13:20	Problemas	11 detectados

B

83/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado sobre el sitio web ha arrojado una puntuacion de 83/100, lo que corresponde a una nota de B. Durante la evaluacion se ejecutaron 9 checks pasivos, identificando que 7 de ellos cumplieron con los estandares de seguridad mientras que 2 presentaron fallos criticos. Aunque la infraestructura de red y el cifrado son solidos, existen deficiencias importantes en la configuracion de cabeceras de proteccion y en la gestion de cookies. Se concluye que el sitio es generalmente seguro para la navegacion, pero vulnerable a ataques especificos de secuestro de sesion e inyeccion de contenido.

Resumen de Riesgos

0	6	2	3	46
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 75 dias
Cabeceras de Seguridad	45	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: Wix
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	44	FALLO	ssr-caching: falta HttpOnly; ssr-caching: falta ...
Contenido Mixto	100	OK	No se detecto contenido mixto
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 75 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  75 dias restantes (expira: 2026-07-19T11:26:49.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-20T11:26:50.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 45/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Pepyaka — 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=31536000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- 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.wix.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Wix

- 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**
  Detectado via HTML body
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Wix.com Website Builder
- INFO **Tecnologias detectadas**
  React, Next.js

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 — 44/100

Estado: FALLO

ssr-caching: falta HttpOnly; ssr-caching: falta Secure; ssr-caching: falta SameSite; _wixCIDX: falta HttpOnly; _wixUIDX: falta HttpOnly

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- ALTO **Cookie: ssr-caching — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: ssr-caching — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: ssr-caching — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: _wixCIDX — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: _wixCIDX — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _wixCIDX — SameSite**
  SameSite=none
- ALTO **Cookie: _wixUIDX — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: _wixUIDX — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _wixUIDX — SameSite**
  SameSite=none

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (2883 bytes)
- INFO **Reglas robots.txt**
  90 Disallow, 0 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.wix.com/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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecucion de scripts no autorizados, aumentando el riesgo de ataques XSS.
[HIGH] X-Frame-Options: Al faltar esta directiva, el sitio puede ser cargado dentro de marcos externos, lo que facilita ataques de clickjacking.
[HIGH] Cookie ssr-caching (HttpOnly): La falta de este flag permite que la cookie sea accesible mediante JavaScript, exponiendo la sesion ante scripts maliciosos.
[HIGH] Cookie ssr-caching (Secure): El atributo Secure no esta presente, lo que podria causar que la cookie se envie a traves de conexiones no cifradas.
[HIGH] Cookie _wixCIDX (HttpOnly): Esta cookie de sesion carece de proteccion contra acceso programatico, permitiendo su posible robo via XSS.
[HIGH] Cookie _wixUIDX (HttpOnly): Al no tener el flag de solo lectura para el protocolo HTTP, se compromete la integridad del identificador de usuario.
[MEDIUM] Permissions-Policy: La falta de esta cabecera impide restringir el uso de APIs del navegador como la camara o el microfono por parte de terceros.
[MEDIUM] Cookie ssr-caching (SameSite): La ausencia de este atributo hace que el sitio sea susceptible a ataques de falsificacion de peticion en sitios cruzados (CSRF).
[LOW] Server header expuesto: Se detecto la cabecera Server con el valor Pepyaka, lo cual revela informacion sobre la tecnologia del servidor a posibles atacantes.
[LOW] Meta generator: El codigo fuente expone que el sitio utiliza Wix.com Website Builder, facilitando el reconocimiento del sistema de gestion de contenidos.
[LOW] Ruta sensible en robots.txt: Se ha encontrado una referencia al directorio config, lo que podria guiar a un atacante hacia archivos de configuracion interna.