EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://vercel.com/	Checks	9 pruebas
Dominio	vercel.com	Hallazgos	55 totales
Fecha	27 de abril de 2026 a las 14:45	Problemas	9 detectados

A

92/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad de vercel.com ha resultado en una puntuacion de 92/100 con una calificacion de nota A. Se ejecutaron 9 checks pasivos que arrojaron 6 resultados satisfactorios y 3 advertencias, sin detectarse ningun fallo critico. Los hallazgos principales se centran en la exposicion de informacion tecnica y la configuracion de cookies de seguimiento. El sitio demuestra una implementacion solida de protocolos de cifrado y transporte de datos. Se concluye que el sitio es seguro, aunque requiere ajustes menores en la gestion de cabeceras y archivos publicos para alcanzar la excelencia en su postura de seguridad.

Resumen de Riesgos

0	3	4	2	46
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 54 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: Permissions-Policy
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	67	AVISO	_v-consent: falta HttpOnly; _v-anonymous-id: fal...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 54 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  54 dias restantes (expira: 2026-06-21T02:21:57.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-23T02:21:58.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: Permissions-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Next.js, Payload — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: default-src 'self' vercel.com *.vercel.com assets.vercel.com *.vercel.sh vercel....
- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: origin-when-cross-origin
- 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 308 redirige a https://vercel.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS 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

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**
  React, Next.js, Nuxt, Astro, Next.js, Payload

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 67/100

Estado: AVISO

_v-consent: falta HttpOnly; _v-anonymous-id: falta HttpOnly; _v-anonymous-id-renewed: falta HttpOnly

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- ALTO **Cookie: _v-consent — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: _v-consent — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _v-consent — SameSite**
  SameSite=lax
- ALTO **Cookie: _v-anonymous-id — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: _v-anonymous-id — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _v-anonymous-id — SameSite**
  SameSite=lax
- ALTO **Cookie: _v-anonymous-id-renewed — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: _v-anonymous-id-renewed — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _v-anonymous-id-renewed — 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 robots.txt

- INFO **sitemap.xml**
  Presente, 4415 URLs
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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

[LOW] Server header expuesto: El servidor responde con la cabecera Server: Vercel, lo que revela la infraestructura subyacente a posibles atacantes.
[LOW] X-Powered-By expuesto: Se divulga el uso de Next.js y Payload, permitiendo identificar el framework para buscar vulnerabilidades especificas.
[MEDIUM] Permissions-Policy faltante: La ausencia de esta cabecera impide restringir el acceso del navegador a funciones sensibles como la camara o el microfono.
[MEDIUM] Archivo /readme.html expuesto: Este archivo es accesible publicamente y podria contener detalles sobre versiones o configuraciones internas del sistema.
[MEDIUM] Archivo /README.txt expuesto: La disponibilidad de este documento facilita la obtencion de metadatos o informacion tecnica del despliegue.
[MEDIUM] Ruta /user/login expuesta: El panel de autenticacion es visible para cualquier usuario, aumentando la superficie de ataque para intentos de acceso no autorizado.
[HIGH] Cookie _v-consent sin HttpOnly: La falta de este atributo permite que la cookie sea accesible mediante scripts, elevando el riesgo de ataques XSS.
[HIGH] Cookie _v-anonymous-id sin HttpOnly: El identificador anonimo puede ser secuestrado por codigo malicioso ejecutado en el lado del cliente.
[HIGH] Cookie _v-anonymous-id-renewed sin HttpOnly: Al igual que las anteriores, esta cookie carece de la proteccion necesaria contra el acceso por Javascript.
[LOW] Ausencia de robots.txt: No existe un archivo de reglas para buscadores, lo que dificulta la gestion del rastreo de rutas privadas.