

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.vintedge.vip/	Checks	9 pruebas
Dominio	www.vintedge.vip	Hallazgos	44 totales
Fecha	11 de abril de 2026 a las 18:13	Problemas	2 detectados

A

93/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja una puntuación técnica de 93/100, lo que le otorga una calificación de grado A. Se han ejecutado 9 chequeos pasivos, obteniendo 7 resultados satisfactorios y 2 advertencias, sin registrarse fallos críticos. La infraestructura muestra una base sólida con una implementación excelente de cifrado SSL y redirecciones seguras de tráfico. En conclusión, el sitio se considera seguro bajo parámetros generales, aunque presenta vulnerabilidades de configuración en sus cabeceras de respuesta que deben ser subsanadas para prevenir ataques de inyección.

Resumen de Riesgos

0 CRITICO	1 ALTO	0 MEDIO	1 BAJO	42 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 33 dias
Cabeceras de Seguridad	75	AVISO	5/6 presentes. Faltan: Content-Security-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	100	OK	No se encontraron cookies
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 33 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
33 dias restantes (expira: 2026-05-14T20:26:23.000Z)
- INFO Fecha de emision
Emitido desde: 2026-02-13T20:26:24.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

5/6 presentes. Faltan: Content-Security-Policy

- BAJO Server header expuesto
Server: Vercel — Revela tecnología del servidor

- ALTO

Content-Security-Policy
Falta — Previene XSS y ataques de inyeccion de contenido
- INFO

X-Frame-Options
Presente: DENY
- INFO

Strict-Transport-Security
Presente: max-age=63072000; includeSubDomains; preload
- INFO

X-Content-Type-Options
Presente: nosniiff
- INFO

Referrer-Policy
Presente: strict-origin-when-cross-origin
- INFO

Permissions-Policy
Presente: camera=(), microphone=(), geolocation=()

Redireccion HTTPS — 100/100

Estado: OK
HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

HTTP !' HTTPS redireccion
HTTP 308 redirige a https://www.vintedge.vip/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=63072000; includeSubDomains; preload
- BAJO

HSTS includeSubDomains
HSTS cubre subdominios
- INFO

HSTS max-age
max-age=63072000 (730 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

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 — 100/100

Estado: OK
No se encontraron cookies

● INFO **Cookies detectadas**
El sitio no establece cookies en la respuesta inicial

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, 23 URLs

● 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 ataques de Cross-Site Scripting (XSS) e inyecciones de contenido al no restringir las fuentes de ejecución de scripts.

[LOW] Server header expuesto: Se detectó la cabecera Server indicando el uso de Vercel, lo cual facilita a un atacante la identificación de la tecnología subyacente y la búsqueda de exploits específicos.

[LOW] Ausencia de archivo robots.txt: No existe un archivo de reglas de rastreo, lo que puede derivar en la indexación de directorios no deseados por parte de motores de búsqueda.