EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://bravodesatascostenerife.com	Checks	9 pruebas
Dominio	bravodesatascostenerife.com	Hallazgos	47 totales
Fecha	28 de abril de 2026 a las 20:04	Problemas	14 detectados

C

67/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al dominio bravodesatascostenerife.com refleja una puntuación de 67/100, lo que otorga una calificación de grado C. El análisis pasivo ejecutó un total de 9 comprobaciones, resultando en 5 verificaciones correctas, 2 advertencias y 2 fallos de seguridad críticos. Aunque el sitio web cuenta con un cifrado de transporte adecuado, se han detectado debilidades importantes en la configuración de cabeceras y la exposición de versiones de software. Por tanto, el sitio se clasifica actualmente como vulnerable, ya que presenta vectores de ataque conocidos que podrían ser explotados por terceros. Se requiere una intervención técnica para mitigar los riesgos identificados y mejorar la postura de seguridad.

Resumen de Riesgos

0	6	5	3	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 79 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
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 6.9.4 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 79 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  79 dias restantes (expira: 2026-07-16T10:58:29.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-17T10:58:30.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: Apache — 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
- 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
- INFO **Permissions-Policy**
  Presente: private-state-token-redemption=(self "https://www.google.com" "https://www.gstat...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://bravodesatascostenerife.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

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 6.9.4
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.9.4 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 — 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 (128 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://bravodesatascostenerife.com/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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] WordPress version: La versión 6.9.4 está expuesta públicamente, lo que permite a atacantes buscar y aplicar exploits para vulnerabilidades conocidas (CVEs).
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques XSS (Cross-Site Scripting) y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: Al faltar esta directiva, el sitio es susceptible a ataques de clickjacking mediante el uso de marcos o iframes.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que significa que el navegador no fuerza la conexión HTTPS, permitiendo ataques de degradación de protocolo.
[HIGH] Puerto 21 (FTP): El puerto de transferencia de archivos está abierto y opera sin cifrado, exponiendo credenciales y datos en tránsito.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que los navegadores realicen sniffing de tipos MIME, aumentando el riesgo de ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se controla la información de referencia que el sitio envía a otros dominios, lo que podría filtrar rutas internas.
[MEDIUM] Archivo /readme.html: Este archivo es accesible de forma pública y revela detalles técnicos y la versión específica del CMS utilizado.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es visible para cualquier usuario, facilitando intentos de acceso por fuerza bruta.
[MEDIUM] Puerto 22 (SSH): Se detectó el puerto de acceso remoto abierto, lo que representa un punto de entrada potencial si no está debidamente protegido.
[LOW] Server header expuesto: El servidor revela que utiliza Apache, proporcionando información técnica valiosa para la fase de reconocimiento de un atacante.
[LOW] Meta generator: La etiqueta meta expone explícitamente el uso de WordPress 6.9.4 en el código fuente de la página.
[LOW] Ruta sensible en robots.txt: El archivo incluye una referencia directa a la carpeta admin, indicando a los atacantes la ubicación de áreas sensibles.