EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.barracudalanzarote.com	Checks	9 pruebas
Dominio	www.barracudalanzarote.com	Hallazgos	46 totales
Fecha	19 de septiembre de 2026 a las 00:23	Problemas	11 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de ciberseguridad realizada al dominio barracudalanzarote.com ha resultado en una puntuacion de 68/100, lo que equivale a una nota de C. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 6 resultados satisfactorios, 1 advertencia relacionada con la redireccion de trafico y 2 fallos criticos en la configuracion del servidor. Aunque el sitio cuenta con un cifrado de datos activo, la falta de politicas de seguridad en las cabeceras HTTP y la exposicion de informacion tecnica lo vuelven vulnerable. En conclusion, el sitio web presenta un estado de seguridad debil que requiere intervencion tecnica para mitigar riesgos de ataques externos.

Resumen de Riesgos

0	5	3	3	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 139 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 1789560140 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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 139 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  139 dias restantes (expira: 2027-02-04T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-25T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: IONOS Webserver — 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
- 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://www.barracudalanzarote.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

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: MyWebsite NOW
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 1789560140 expuesta

- ALTO **WordPress version**
  Version 1789560140 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)

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 (127 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://www.barracudalanzarote.com/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] WordPress version expuesta: La version 1789560140 es visible publicamente, lo que permite a atacantes identificar vulnerabilidades especificas (CVEs) para este software.
[HIGH] Content-Security-Policy ausente: La falta de esta cabecera permite ataques de inyeccion de contenido y Cross-Site Scripting (XSS) al no restringir el origen de los recursos.
[HIGH] X-Frame-Options ausente: Sin esta proteccion, el sitio es susceptible a ataques de clickjacking, donde un atacante puede cargar la web en un marco invisible para engañar al usuario.
[HIGH] Strict-Transport-Security (HSTS) no configurado: El servidor no ordena al navegador el uso exclusivo de HTTPS, permitiendo posibles ataques de degradacion de protocolo.
[MEDIUM] X-Content-Type-Options ausente: El sitio no previene el MIME-type sniffing, lo que podria causar que el navegador interprete archivos de forma insegura.
[MEDIUM] Referrer-Policy ausente: No existe un control sobre la informacion de referencia enviada a otros dominios, lo que podria filtrar rutas internas a terceros.
[MEDIUM] Permissions-Policy ausente: No se restringe el uso de funciones del navegador como la camara o el microfono, aumentando la superficie de ataque en el cliente.
[LOW] Cabecera de servidor expuesta: El valor Server: IONOS Webserver revela informacion sobre la infraestructura que facilita el reconocimiento por parte de atacantes.
[LOW] Meta generator expuesto: La etiqueta revela el uso de MyWebsite NOW, aportando datos adicionales sobre las herramientas de desarrollo empleadas.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a rutas administrativas, lo cual orienta a los atacantes hacia los puntos de acceso de gestion del sitio.