EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.barracudalanzarote.es	Checks	9 pruebas
Dominio	www.barracudalanzarote.es	Hallazgos	15 totales
Fecha	19 de septiembre de 2026 a las 00:17	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio barracudalanzarote.es arroja una puntuación de 73/100 con una calificación de nota C. Durante la evaluación pasiva se ejecutaron 9 checks, resultando en 1 validación correcta, 0 advertencias y 1 fallo crítico principal que compromete la integridad del análisis detallado. Debido a la imposibilidad de verificar protocolos de cifrado y cabeceras de protección, el sitio no puede considerarse seguro en su estado actual. La ausencia de un pentest activo limita la visibilidad sobre vulnerabilidades de explotación profunda, pero los fallos estructurales detectados son suficientes para clasificar el entorno como vulnerable.

Resumen de Riesgos

1	0	0	2	12
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
  No se pudo establecer conexion SSL/TLS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  Error al acceder
- BAJO **sitemap.xml**
  Error al acceder

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  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

[CRITICAL] Conexión SSL/TLS: No se pudo establecer una conexión segura, lo que impide el cifrado de la información y expone los datos de los usuarios a interceptaciones.
[HIGH] Cabeceras de Seguridad: El servidor no entrega cabeceras HTTP de protección, dejando el sitio expuesto a ataques de clickjacking, XSS e inyección de código.
[HIGH] Redirección HTTPS: La ausencia de una redirección forzada hacia protocolos seguros permite que los atacantes degraden la conexión de los visitantes.
[MEDIUM] Seguridad de Cookies: No se pudo confirmar el uso de atributos Secure o HttpOnly, facilitando el robo de sesiones mediante scripts maliciosos.
[MEDIUM] Contenido Mixto: Existe el riesgo de que elementos del sitio se carguen mediante conexiones no cifradas, rompiendo la cadena de confianza del navegador.
[LOW] Robots.txt y Sitemap: La falta de estos archivos críticos dificulta la gestión de indexación y puede exponer directorios que no deberían ser públicos.
[LOW] Detección de CMS: La incapacidad de identificar el motor del sitio sugiere una configuración de servidor inusual o restrictiva que complica la auditoría de parches conocidos.