EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://bombadur.com.ar	Checks	9 pruebas
Dominio	bombadur.com.ar	Hallazgos	35 totales
Fecha	4 de abril de 2026 a las 22:43	Problemas	4 detectados

B

83/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el sitio obtuvo una puntuación de 83/100 con una calificación final de nota B. Durante el proceso se ejecutaron 9 checks pasivos, resultando en 3 validaciones correctas, 3 advertencias de seguridad y 0 fallos críticos de ejecución. A pesar de la puntuación numérica positiva, la infraestructura revela debilidades estructurales importantes en la exposición de servicios internos. Se concluye que el sitio es actualmente vulnerable debido a configuraciones de red inseguras y falta de políticas de transporte estricto. La presencia de servicios de base de datos abiertos al exterior representa un riesgo inaceptable para la integridad de la plataforma.

Resumen de Riesgos

1	3	0	0	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	83	AVISO	XSRF-TOKEN: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://bombadur.com.ar/
- 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

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**
  Next.js, PHP/8.2.30

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 — 83/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: bombadur_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: bombadur_session — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: bombadur_session — SameSite**
  SameSite=lax

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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] HSTS (Strict-Transport-Security): No se ha configurado esta cabecera, lo que impide que el navegador fuerce conexiones cifradas y permite ataques de degradación de protocolo.
[HIGH] Cookie XSRF-TOKEN: La cookie carece del atributo HttpOnly, lo que permite que sea accesible a través de scripts del lado del cliente y facilita ataques de robo de sesión mediante XSS.
[HIGH] Puerto 21 (FTP) abierto: El servicio de transferencia de archivos está expuesto públicamente, lo que implica un riesgo de interceptación de credenciales y datos al viajar sin cifrado.
[CRITICAL] Puerto 3306 (MySQL) abierto: La base de datos es accesible directamente desde internet, permitiendo intentos de conexión no autorizados o ataques de fuerza bruta contra el motor de datos.