

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://baloncestoandalucia.org
Dominio baloncestoandalucia.org
Fecha 17 de mayo de 2026 a las 17:46

Checks 9 pruebas
Hallazgos 16 totales
Problemas 4 detectados

D

47/100

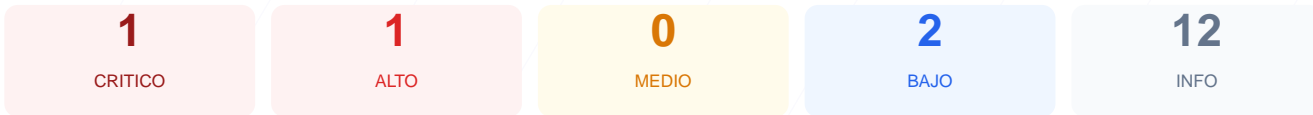
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado al dominio ha dado como resultado una puntuación de 47/100, lo que corresponde a una calificación de nota D. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales se registraron un fallo crítico y una advertencia de seguridad importante. La imposibilidad de verificar el cifrado SSL y la presencia de servicios de transferencia de archivos inseguros comprometen la integridad del sitio. Debido a estas deficiencias estructurales en la configuración del servidor, el sitio se clasifica actualmente como vulnerable.

Resumen de Riesgos



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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

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

Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- INFO** HTTP !' HTTPS redireccion
HTTP 301 redirige a https://www.andaluzabalconcesto.org/

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 — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- **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 — Envío 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 autenticación 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] Conexion SSL/TLS: No se pudo establecer una conexion segura con el servidor, lo que impide el cifrado de los datos y expone la informacion de los usuarios.

[HIGH] Puerto 21 (FTP) Abierto: El servicio de transferencia de archivos FTP esta expuesto y transmite datos y credenciales en texto plano sin cifrar.

[MEDIUM] Cabeceras de Seguridad Ausentes: No se detectaron cabeceras de proteccion, lo que facilita ataques de interceptacion y manipulacion de contenido.

[LOW] Ausencia de robots.txt y sitemap.xml: El servidor devuelve errores al intentar acceder a estos archivos, afectando la indexacion y el control de acceso a directorios.