EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://trofeofutboldiputaciondeburgos.com/	Checks	9 pruebas
Dominio	trofeofutboldiputaciondeburgos.com	Hallazgos	45 totales
Fecha	2 de septiembre de 2026 a las 06:58	Problemas	11 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar una auditoría de ciberseguridad en trofeofutboldiputaciondeburgos.com, el sitio ha obtenido una puntuación de 80/100 con una nota final de B. Durante el análisis se ejecutaron 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 presentaron fallos críticos relacionados con la configuración del servidor. El portal demuestra una implementación sólida de cifrado SSL y transporte seguro de datos. Sin embargo, la ausencia de cabeceras de seguridad y la exposición de archivos internos representan un riesgo moderado. Se concluye que el sitio es generalmente seguro para el usuario final, pero vulnerable a ataques dirigidos de inyección y reconocimiento técnico.

Resumen de Riesgos

0	2	8	1	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 58 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 58 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  58 dias restantes (expira: 2026-10-30T09:53:51.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-01T09:53:52.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: Netlify — 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
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://trofeofutboldiputaciondeburgos.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados, aumentando el riesgo de ataques XSS y robo de datos.

[HIGH] X-Frame-Options: Al no estar configurada, el sitio puede ser cargado dentro de marcos externos, facilitando ataques de clickjacking para engañar a los usuarios.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite al navegador adivinar el tipo de contenido, lo que puede derivar en la ejecución de archivos maliciosos camuflados.
[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada a otros dominios, lo que podría filtrar rutas internas privadas.
[MEDIUM] Permissions-Policy: La carencia de esta política no restringe el acceso a funciones del hardware o APIs del navegador por parte de terceros.
[MEDIUM] Archivos sensibles expuestos: El acceso público a /readme.html y /README.txt permite a un atacante obtener detalles técnicos sobre la infraestructura.
[MEDIUM] Rutas administrativas visibles: La disponibilidad de rutas como /wp-login.php o /administrator/ facilita intentos de acceso no autorizado mediante fuerza bruta.
[LOW] Cabecera Server expuesta: El servidor revela el uso de Netlify, proporcionando información útil para que un atacante identifique vulnerabilidades específicas de la plataforma.
[LOW] Ausencia de robots.txt y sitemap.xml: La falta de estos archivos dificulta la auditoría de indexación y el control sobre qué partes del sitio deben ser rastreadas.