EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.vueltaburgos.com/es	Checks	9 pruebas
Dominio	www.vueltaburgos.com	Hallazgos	43 totales
Fecha	2 de septiembre de 2026 a las 07:00	Problemas	15 detectados

D

44/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha arrojado una puntuación de 44/100, lo que resulta en una nota D. Se han ejecutado 9 checks pasivos, identificando 3 resultados satisfactorios, 1 advertencia y 5 fallos de seguridad críticos. Los hallazgos revelan la exposición de servicios internos del servidor y el uso de software con versiones extremadamente obsoletas. Debido a la falta de políticas de seguridad modernas y la apertura de puertos de bases de datos a internet, se concluye que el sitio es vulnerable y presenta un riesgo alto de compromiso.

Resumen de Riesgos

1	7	4	3	28
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 63 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 2.3.7 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 63 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  63 dias restantes (expira: 2026-11-04T01:16:12.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-06T01:16:13.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: HTTPd — 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)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 0/100

Estado: FALLO
No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO
WordPress 2.3.7 expuesta

- ALTO **WordPress version**
  Version 2.3.7 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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://burgosalimenta.com

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL) abierto: La base de datos del sitio se encuentra expuesta públicamente, permitiendo intentos de conexión externa y ataques de fuerza bruta.
[HIGH] Versión de WordPress 2.3.7 expuesta: El uso de una versión del CMS tan antigua permite a atacantes explotar múltiples vulnerabilidades conocidas y documentadas (CVEs).
[HIGH] Falta de redirección HTTP a HTTPS: El sitio responde a través de conexiones no cifradas, lo que expone los datos de los usuarios a intercepciones.
[HIGH] Content-Security-Policy (CSP) ausente: La falta de esta política facilita la ejecución de ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options ausente: El sitio no cuenta con protección contra ataques de clickjacking, permitiendo que la web sea cargada dentro de marcos maliciosos.

[HIGH] Strict-Transport-Security (HSTS) ausente: El servidor no instruye a los navegadores a utilizar exclusivamente conexiones seguras HTTPS.
[HIGH] Puerto 21 (FTP) abierto: Este servicio de transferencia de archivos es inseguro por naturaleza al transmitir credenciales sin cifrado.
[MEDIUM] Contenido mixto detectado: Se carga una hoja de estilo mediante el protocolo inseguro HTTP desde el dominio burgosalimenta.com dentro de la web protegida.
[MEDIUM] Puerto 22 (SSH) abierto: El servicio de administración remota es visible para cualquier usuario en internet, aumentando la superficie de ataque.
[MEDIUM] Referrer-Policy y Permissions-Policy ausentes: No se controla la información de referencia enviada a otros sitios ni se restringen las APIs sensibles del navegador.
[LOW] Cabecera de servidor expuesta: El servidor revela el uso de HTTPd, lo que facilita la fase de reconocimiento de un atacante para buscar fallos específicos.
[LOW] Archivos robots.txt y sitemap.xml no encontrados: La ausencia de estos archivos dificulta la gestión adecuada del rastreo y la indexación del sitio.