EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.centrosbeup.es/bec/participantes-feria-bec/es/	Checks	9 pruebas
Dominio	www.centrosbeup.es	Hallazgos	49 totales
Fecha	9 de abril de 2026 a las 11:35	Problemas	18 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre el activo digital ha arrojado una puntuación de 64/100, lo que equivale a una calificación de nota C. Durante el análisis se ejecutaron 9 checks pasivos, identificando 5 verificaciones correctas, 2 advertencias y 2 fallos de seguridad críticos. El sistema presenta carencias importantes en la implementación de políticas de seguridad del lado del servidor y una exposición innecesaria de información técnica. Tras evaluar los resultados, se concluye que el sitio es vulnerable ante ataques dirigidos que busquen explotar versiones de software desactualizadas o falta de protecciones en las cabeceras de red.

Resumen de Riesgos

0	6	9	3	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 31 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 5.9.13 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 31 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  31 dias restantes (expira: 2026-05-10T05:00:45.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-09T05:00:46.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PleskLin — Revela framework/lenguaje
- 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)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.centrosbeup.es/
- 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
- BAJO **Meta generator**
  Expone: WordPress 5.9.13
- INFO **Tecnologias detectadas**
  Next.js, PleskLin

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 5.9.13 expuesta

- ALTO **WordPress version**
  Version 5.9.13 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- 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

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (61 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://www.centrosbeup.es/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- 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
- 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] WordPress version: La versión 5.9.13 se encuentra expuesta públicamente, permitiendo a atacantes identificar y explotar CVEs conocidos para este software.
[HIGH] Content-Security-Policy: Falta esta cabecera esencial para prevenir ataques de Cross-Site Scripting (XSS) e inyecciones de contenido.
[HIGH] X-Frame-Options: La ausencia de esta configuración hace al sitio susceptible a ataques de Clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, por lo que el navegador no fuerza el uso de HTTPS, facilitando ataques de degradación de conexión.
[HIGH] Puerto 21 (FTP): El puerto se encuentra abierto, lo que implica transferencia de archivos y credenciales sin cifrar a través de la red.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador realice sniffing de tipos MIME, aumentando el riesgo de ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada en las peticiones salientes.
[MEDIUM] Permissions-Policy: No se restringen las APIs sensibles del navegador como la cámara o el micrófono.
[MEDIUM] Archivos informativos expuestos: Los archivos /readme.html y /README.txt son accesibles y revelan detalles técnicos de la instalación.
[MEDIUM] Rutas administrativas visibles: Los paneles de login en /wp-login.php, /administrator/ y /user/login son accesibles para cualquier usuario de internet.
[MEDIUM] Puerto 22 (SSH): El puerto de acceso remoto está abierto, representando un vector de ataque si no posee restricciones de IP o autenticación robusta.
[WARN] Redirección HTTPS incompleta: El tráfico HTTP redirige a HTTPS, pero la ausencia de HSTS debilita esta protección.
[LOW] Cabecera Server expuesta: Revela el uso de tecnología nginx, facilitando la fase de reconocimiento de un atacante.
[LOW] Cabecera X-Powered-By expuesta: Indica el uso de PleskLin como framework o panel de gestión.
[LOW] Meta generator visible: Confirma explícitamente el uso de WordPress 5.9.13 en el código fuente.