EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.crossatapuerca.com/nw	Checks	9 pruebas
Dominio	www.crossatapuerca.com	Hallazgos	44 totales
Fecha	2 de septiembre de 2026 a las 07:01	Problemas	14 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web analizado presenta una puntuación de seguridad de 59/100, lo que resulta en una calificación de nota D. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 3 resultaron satisfactorios, 3 generaron advertencias y 3 fueron fallos críticos de seguridad. Se han identificado riesgos importantes relacionados con la exposición de versiones de software obsoletas y la falta de configuraciones de protección en el servidor. Debido a la combinación de servicios inseguros abiertos y la ausencia de cabeceras de seguridad esenciales, se concluye que el sitio es actualmente vulnerable a diversos vectores de ataque. Es necesaria una intervención técnica inmediata para mitigar los riesgos detectados y proteger la integridad de la plataforma.

Resumen de Riesgos

0	6	4	4	30
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	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 4.13.10 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	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

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: 2026-11-04T01:15:47.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-06T01:15:48.000Z
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.crossatapuerca.com/nw/
- 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, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Powered by WPBakery Page Builder - drag and drop page builder for WordPress.
- INFO **Tecnologias detectadas**
  Next.js, Astro

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 4.13.10 expuesta

- ALTO **WordPress version**
  Version 4.13.10 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://atapuerca.burgos.es/

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 — 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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: El sitio expone públicamente la versión 4.13.10 de WordPress, lo cual permite a atacantes identificar y explotar vulnerabilidades conocidas (CVE) para este software obsoleto.
[HIGH] Content-Security-Policy: Falta de cabecera CSP, lo que deja el sitio desprotegido frente a ataques de Cross-Site Scripting (XSS) e inyecciones de contenido malicioso.

[HIGH] X-Frame-Options: La ausencia de esta cabecera facilita ataques de clickjacking, permitiendo que el sitio sea embebido en marcos invisibles para engañar a los usuarios.
[HIGH] Strict-Transport-Security: No se ha configurado la política HSTS, por lo que el navegador no fuerza conexiones seguras de manera persistente, permitiendo posibles ataques de degradación de protocolo.
[HIGH] Puerto 21 (FTP): Se detectó el puerto 21 abierto, lo que implica la transferencia de archivos y credenciales de administración sin cifrado a través de la red.
[MEDIUM] Contenido Mixto: Se detectó un recurso stylesheet cargado mediante el protocolo inseguro HTTP desde el dominio atapuerca.burgos.es, debilitando el cifrado general de la página.
[MEDIUM] Referrer-Policy: El servidor no controla qué información de procedencia se envía a terceros al navegar desde el sitio, lo que puede derivar en fugas de información.
[MEDIUM] Permissions-Policy: La falta de esta política impide restringir el uso de APIs sensibles del navegador como la cámara, el micrófono o la geolocalización por parte de terceros.
[MEDIUM] Puerto 22 (SSH): El puerto de acceso remoto se encuentra abierto, lo que incrementa la superficie de exposición ante intentos de acceso no autorizado mediante fuerza bruta.
[LOW] Server header expuesto: El encabezado del servidor revela el uso de HTTPd, proporcionando información técnica valiosa a posibles atacantes durante la fase de reconocimiento.
[LOW] Meta generator: La presencia de metadatos sobre WPBakery Page Builder confirma herramientas de diseño específicas que pueden ser objeto de ataques dirigidos.
[LOW] Robots.txt y Sitemap: La ausencia de estos archivos dificulta la correcta indexación y puede ocultar errores de estructura interna del sitio web.