EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://circoraluy.com	Checks	9 pruebas
Dominio	circoraluy.com	Hallazgos	47 totales
Fecha	23 de abril de 2026 a las 14:01	Problemas	17 detectados

D

49/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado en circoraluy.com arroja una puntuación de 49/100, lo que equivale a una calificación de grado D. Se ejecutaron 9 comprobaciones pasivas, resultando en 5 satisfactorias y 4 fallos críticos, sin la realización de un pentest activo. Los hallazgos revelan deficiencias graves en la configuración de cabeceras de seguridad y una exposición peligrosa de puertos de infraestructura. La ausencia de redirección HTTPS y la visibilidad de versiones de software obsoletas incrementan significativamente la superficie de ataque. En su estado actual, el sitio web se considera vulnerable y presenta un riesgo elevado para la integridad de los datos.

Resumen de Riesgos

1	7	6	3	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 90 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.9.4 expuesta, WordPress 2 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	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 90 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  90 dias restantes (expira: 2026-07-22T02:28:31.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-23T02:28:32.000Z
- 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: 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)
- 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 — 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, 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: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.9.4 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

- MEDIO **Ruta /wp-login.php**
  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 (520 bytes)
- INFO **Reglas robots.txt**
  8 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://circoraluy.com/sitemap_index.xml
- 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): El servicio de base de datos está abierto al exterior, permitiendo intentos de conexión directa.
[HIGH] Content-Security-Policy (CSP): Falta esta cabecera esencial que previene ataques de inyección de código y XSS.
[HIGH] X-Frame-Options: Cabecera ausente, lo que hace al sitio susceptible a ataques de secuestro de clics o clickjacking.
[HIGH] Strict-Transport-Security (HSTS): No se fuerza el uso de HTTPS, permitiendo comunicaciones interceptables.
[HIGH] Redireccion HTTP a HTTPS: El sitio no redirige automáticamente el tráfico inseguro al protocolo seguro.
[HIGH] WordPress version 6.9.4: La versión del CMS está expuesta y desactualizada, facilitando la búsqueda de exploits conocidos.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos abierto que transmite credenciales y datos sin cifrar.
[MEDIUM] X-Content-Type-Options: Falta la cabecera para evitar que el navegador interprete archivos con tipos MIME incorrectos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación que se envía a otros sitios.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador como la cámara o el micrófono.
[MEDIUM] Archivo /readme.html y /wp-login.php: Archivos y rutas de administración accesibles que revelan información técnica.
[MEDIUM] Puerto 22 (SSH): Acceso remoto abierto, lo que permite ataques de fuerza bruta contra el servidor.
[LOW] Server header expuesto: El servidor informa que usa HTTPd, ayudando a los atacantes a perfilar el sistema.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a rutas de administración, guiando a posibles intrusos.