EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Jp.org.pe	Checks	9 pruebas
Dominio	jp.org.pe	Hallazgos	48 totales
Fecha	21 de mayo de 2026 a las 02:47	Problemas	9 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 76/100, lo que equivale a una calificación de nota B. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 7 resultaron satisfactorias y 2 presentaron fallos críticos de configuración. Aunque el cifrado de datos es robusto, la exposición de versiones de software y la falta de cabeceras de seguridad defensivas elevan el riesgo técnico. Se concluye que el sitio es actualmente vulnerable a ataques de inyección de scripts y suplantación de interfaz. Es imperativo corregir las deficiencias en las políticas de seguridad del navegador para mejorar la resiliencia del portal.

Resumen de Riesgos

0	3	3	3	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 56 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	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 20211021 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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 56 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  56 dias restantes (expira: 2026-07-16T06:56:26.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-17T06:56:27.000Z
- 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: nginx — 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://jp.org.pe/
- 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

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.com
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 20211021 expuesta

- ALTO **WordPress version**
  Version 20211021 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 — 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 (618 bytes)
- INFO **Reglas robots.txt**
  10 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://jp.org.pe/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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] WordPress version: La versión 20211021 está expuesta públicamente, lo que permite a atacantes identificar y explotar vulnerabilidades conocidas (CVEs) de esa versión específica.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera impide prevenir ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso en el navegador del usuario.
[HIGH] X-Frame-Options: No se detectó esta cabecera, dejando el sitio desprotegido contra ataques de Clickjacking que podrían engañar a los usuarios para realizar acciones no deseadas.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite el MIME-type sniffing, lo que podría llevar a la ejecución de archivos maliciosos disfrazados de elementos inofensivos.
[MEDIUM] Referrer-Policy: No existe un control sobre la información de referencia enviada a otros sitios, lo que puede filtrar datos privados de la estructura de navegación.
[MEDIUM] Permissions-Policy: Falta esta configuración para restringir el acceso del navegador a APIs sensibles como la cámara, el micrófono o la geolocalización.
[LOW] Server header expuesto: El encabezado revela el uso del servidor Nginx, proporcionando información valiosa a un atacante sobre la infraestructura tecnológica.
[LOW] Meta generator: El código fuente expone que el sitio utiliza WordPress.com, facilitando el reconocimiento de la plataforma por parte de agentes externos.
[LOW] Ruta sensible en robots.txt: Se hace referencia explícita a la ruta admin, lo que orienta a posibles atacantes hacia los puntos de entrada de la gestión administrativa.