EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://radielloperu.com/	Checks	9 pruebas
Dominio	radielloperu.com	Hallazgos	38 totales
Fecha	9 de septiembre de 2026 a las 19:22	Problemas	9 detectados

C

71/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre radielloperu.com ha dado como resultado una puntuación de 71/100, lo que equivale a una nota de C. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 5 resultados satisfactorios, 1 advertencia y 1 fallo crítico en la configuración de cabeceras. Aunque la comunicación básica está cifrada, la ausencia de protecciones avanzadas en el servidor representa un riesgo latente. Debido a la carencia total de políticas de seguridad en las respuestas HTTP, el sitio se considera actualmente vulnerable ante ataques de inyección y suplantación. Se requiere una intervención inmediata para elevar los estándares de protección de la plataforma.

Resumen de Riesgos

0	4	3	2	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 56 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
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

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: 2026-11-04T20:53:34.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-06T20:53:35.000Z
- 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: Apache — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://radielloperu.com/
- 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 7.1
- INFO **Tecnologias detectadas**
  React, Next.js, Astro

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

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  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] Content-Security-Policy: Falta la cabecera que previene ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Ausencia de protección contra clickjacking, permitiendo que el sitio sea embebido en marcos maliciosos.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide obligar al navegador a usar siempre conexiones seguras.
[MEDIUM] X-Content-Type-Options: El servidor no previene el MIME-type sniffing, facilitando la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Referrer-Policy: Falta de control sobre la información de navegación que se envía a otros dominios mediante el referer.
[MEDIUM] Permissions-Policy: No se restringe el acceso de las APIs del navegador a componentes sensibles como cámara o micrófono.
[LOW] Server header expuesto: La cabecera revela el uso de Apache, proporcionando información útil para atacantes sobre la tecnología del servidor.
[LOW] Meta generator: El sitio expone públicamente que utiliza WordPress versión 7.1, facilitando la búsqueda de exploits específicos.