EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://catalejo.rf.gd	Checks	9 pruebas
Dominio	catalejo.rf.gd	Hallazgos	44 totales
Fecha	30 de abril de 2026 a las 12:52	Problemas	15 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar la auditoría de seguridad en el sitio web, se ha obtenido una puntuación de 57/100, lo que equivale a una nota D. El análisis se basó en 9 checks pasivos, de los cuales 5 resultaron satisfactorios, se emitió 1 advertencia y se detectaron 3 fallos críticos en la configuración. Debido a la carencia total de cabeceras de seguridad y a la falta de redirección forzada hacia conexiones cifradas, se concluye que el sitio es actualmente vulnerable. Es imperativo realizar ajustes técnicos para mitigar riesgos de ataques comunes que comprometen la integridad de la navegación.

Resumen de Riesgos

0	5	8	2	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	70	AVISO	Certificado expira en 21 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 70/100

Estado: AVISO

Certificado expira en 21 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- MEDIO **Dias hasta expiracion**
  21 dias restantes (expira: 2026-05-21T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-20T00:00:00.000Z
- 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: openresty — 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

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- 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

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- 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

- INFO **Version CMS**
  No se detecta ninguna version expuesta

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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] Content-Security-Policy: Falta esta cabecera esencial para prevenir ataques de Cross-Site Scripting (XSS) e inyecciones de contenido.
[HIGH] X-Frame-Options: Su ausencia permite ataques de clickjacking, donde un atacante puede inducir al usuario a realizar acciones no deseadas.
[HIGH] Strict-Transport-Security: No se fuerza el protocolo HSTS, permitiendo que el navegador establezca conexiones no seguras.
[HIGH] Redirección HTTP a HTTPS: El sitio permite el acceso por el puerto 80 sin redirigir al usuario automáticamente a la versión cifrada.

[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que puede ser explotado para ejecutar scripts maliciosos.
[MEDIUM] Referrer-Policy: No hay control sobre la información que el navegador envía al navegar hacia otros enlaces externos.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, dejando expuestos componentes como la cámara o el micrófono.
[MEDIUM] Archivos Informativos Expuestos: Se detectó acceso público a archivos /readme.html y /README.txt que pueden revelar detalles del sistema.
[MEDIUM] Paneles de Administración Expuestos: Las rutas /wp-login.php, /administrator/ y /user/login son accesibles, facilitando intentos de fuerza bruta.
[LOW] Servidor Expuesto: La cabecera Server revela el uso de openresty, proporcionando información técnica útil para un posible atacante.
[LOW] SSL con Caducidad Próxima: El certificado SSL actual expira en 21 días, lo que representa un riesgo para la disponibilidad segura del sitio.
[LOW] Ausencia de Robots.txt y Sitemap: La falta de estos archivos impide una correcta gestión del rastreo y visibilidad en buscadores.