

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://Wikipedia.com
Dominio wikipedia.com
Fecha 27 de mayo de 2026 a las 18:39

Checks 9 pruebas
Hallazgos 62 totales
Problemas 13 detectados

B

81/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio ha resultado en una puntuación de 81/100, lo que equivale a una nota B. Se ejecutaron un total de 9 comprobaciones pasivas, obteniendo 7 resultados satisfactorios, 1 advertencia en la gestión de cookies y 1 fallo crítico en la configuración de cabeceras de seguridad. El sitio presenta una base sólida en cuanto a cifrado y certificados, pero carece de protecciones modernas contra ataques de inyección y suplantación. Se concluye que el sitio es moderadamente seguro, aunque técnicamente vulnerable a vectores de ataque específicos debido a configuraciones de servidor incompletas.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 57 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	67	AVISO	WMF-Last-Access: falta SameSite; WMF-Last-Access...
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 57 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
57 dias restantes (expira: 2026-07-23T20:00:29.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-24T20:00:30.000Z
- 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: ATS/9.2.13 — 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=106384710; includeSubDomains; preload
- **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://wikipedia.com/
- **INFO** **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=106384710; includeSubDomains; preload
- **BAJO** **HSTS includeSubDomains**
HSTS cubre subdominios
- **INFO** **HSTS max-age**
max-age=106384710 (1231 dias)
- **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

- **INFO** **Archivo /readme.html**
No accesible (correcto)
- **INFO** **Archivo /README.txt**
No accesible (correcto)
- **INFO** **Version CMS**
No se detecta ninguna version expuesta

Seguridad de Cookies — 67/100

Estado: AVISO

WMF-Last-Access: falta SameSite; WMF-Last-Access-Global: falta SameSite; GeolIP: falta HttpOnly; GeolIP: falta SameSite; NetworkProbeLimit: falta HttpOnly

- **INFO** **Cookies detectadas**
5 cookie(s) encontrada(s)
- **INFO** **Cookie: WMF-Last-Access — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- **INFO** **Cookie: WMF-Last-Access — Secure**
Flag Secure activo — Solo se envía por HTTPS
- **MEDIO** **Cookie: WMF-Last-Access — SameSite**
Falta SameSite — Vulnerable a CSRF
- **INFO** **Cookie: WMF-Last-Access-Global — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- **INFO** **Cookie: WMF-Last-Access-Global — Secure**
Flag Secure activo — Solo se envía por HTTPS
- **MEDIO** **Cookie: WMF-Last-Access-Global — SameSite**
Falta SameSite — Vulnerable a CSRF
- **ALTO** **Cookie: GeolIP — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- **INFO** **Cookie: GeolIP — Secure**
Flag Secure activo — Solo se envía por HTTPS
- **MEDIO** **Cookie: GeolIP — SameSite**
Falta SameSite — Vulnerable a CSRF
- **ALTO** **Cookie: NetworkProbeLimit — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- **INFO** **Cookie: NetworkProbeLimit — Secure**
Flag Secure activo — Solo se envía por HTTPS
- **INFO** **Cookie: NetworkProbeLimit — SameSite**
SameSite=none
- **INFO** **Cookie: WMF-Uniq — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- **INFO** **Cookie: WMF-Uniq — Secure**
Flag Secure activo — Solo se envía por HTTPS
- **INFO** **Cookie: WMF-Uniq — SameSite**
SameSite=none

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 (28027 bytes)
- **INFO** **Reglas robots.txt**
460 Disallow, 4 Allow
- **MEDIO** **Bloqueo total**
robots.txt bloquea todo el sitio con Disallow: /
- **BAJO** **Ruta sensible en robots.txt**
Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- **INFO** **Sitemap en robots.txt**
<https://en.wikipedia.org/w/rest.php/site/v1/sitemap/0>

- 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 — Envío 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: La ausencia de esta cabecera permite la ejecución de ataques XSS y la inyección de contenido malicioso.

[HIGH] X-Frame-Options: Al no estar presente, el portal es susceptible a ataques de clickjacking que podrían engañar a los usuarios.

[HIGH] Cookie GeolP (HttpOnly): La falta de esta bandera permite que la cookie sea accesible mediante scripts del navegador, facilitando ataques XSS.

[HIGH] Cookie NetworkProbeLimit (HttpOnly): El acceso vía JavaScript a esta cookie representa un riesgo elevado de robo de información de sesión.

[MEDIUM] X-Content-Type-Options: El servidor no bloquea el olfateo de tipos MIME, lo que permite que el navegador interprete archivos de forma insegura.

[MEDIUM] Referrer-Policy: No se controla la cantidad de información que el navegador envía al navegar hacia enlaces externos.

[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono.

[MEDIUM] Cookies (SameSite): Las cookies WMF-Last-Access, WMF-Last-Access-Global y GeolP carecen del atributo SameSite, haciéndolas vulnerables a ataques CSRF.

[MEDIUM] robots.txt: El archivo bloquea la indexación total y revela la existencia de una ruta administrativa, lo cual es útil para el reconocimiento de un atacante.

[LOW] Server header expuesto: El servidor revela el uso de ATS/9.2.13, proporcionando información técnica valiosa para la planificación de exploits específicos.