EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.wikipedia.org/	Checks	9 pruebas
Dominio	www.wikipedia.org	Hallazgos	62 totales
Fecha	20 de mayo de 2026 a las 21:41	Problemas	13 detectados

B

81/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio analizado arroja una puntuación de 81/100 con una calificación de B. Se ejecutaron un total de 9 comprobaciones pasivas, resultando en 7 verificaciones exitosas, 1 advertencia y 1 fallo crítico en la configuración de cabeceras. La infraestructura presenta una base sólida en cuanto a cifrado y conectividad, pero muestra carencias importantes en las políticas de seguridad del navegador y la protección de cookies. En conclusión, el sitio web es mayoritariamente seguro, aunque presenta vulnerabilidades de severidad media y alta que deben ser corregidas para prevenir ataques de inyección y suplantación.

Resumen de Riesgos

0	4	7	2	49
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 47 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 47 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  47 dias restantes (expira: 2026-07-06T20:52:29.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-07T20:52:30.000Z
- 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://www.wikipedia.org/
- 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; GeoIP: falta HttpOnly; GeoIP: 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 envia 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 envia por HTTPS
- MEDIO **Cookie: WMF-Last-Access-Global — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: GeoIP — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: GeoIP — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: GeoIP — 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 envia 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 envia 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 — 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: La ausencia de esta cabecera permite la ejecución de scripts no autorizados y ataques de Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Al no estar presente, el sitio es vulnerable a ataques de clickjacking, permitiendo que sea cargado en marcos externos maliciosos.
[HIGH] Cookie GeoIP (HttpOnly): La falta del atributo HttpOnly permite que la cookie sea accesible mediante JavaScript, aumentando el riesgo de robo de información en caso de XSS.
[HIGH] Cookie NetworkProbeLimit (HttpOnly): Esta cookie carece de protección contra acceso por script, lo que facilita la exfiltración de datos técnicos de la sesión.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que podría llevar al navegador a ejecutar archivos con contenido malicioso disfrazado.
[MEDIUM] Referrer-Policy: No se ha definido una política para el envío de información de procedencia, lo que puede filtrar datos de navegación a sitios externos.
[MEDIUM] Permissions-Policy: La ausencia de esta configuración impide restringir el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[MEDIUM] Atributo SameSite en Cookies: Las cookies WMF-Last-Access, WMF-Last-Access-Global y GeoIP no tienen definido el atributo SameSite, lo que las hace vulnerables a ataques de Cross-Site Request Forgery (CSRF).
[MEDIUM] Bloqueo total en robots.txt: La directiva de bloqueo total puede ocultar comportamientos anómalos o dificultar la auditoría legítima de rutas públicas.
[LOW] Server header expuesto: La cabecera Server revela el uso de ATS/9.2.13, proporcionando a potenciales atacantes información valiosa sobre la tecnología y versión del servidor.
[LOW] Ruta sensible en robots.txt: La mención de la ruta "admin" en el archivo de rastreo facilita la enumeración de directorios privados por parte de agentes malintencionados.