EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://es.wikipedia.org/wiki/Wikipedia:Portada	Checks	9 pruebas
Dominio	es.wikipedia.org	Hallazgos	63 totales
Fecha	20 de mayo de 2026 a las 21:32	Problemas	12 detectados

B

89/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio arroja una puntuación de 89/100 con una nota final de B. Se han ejecutado un total de 9 comprobaciones pasivas, de las cuales 7 resultaron satisfactorias, una presenta advertencias de configuración y otra ha fallado debido a la ausencia de protecciones esenciales. El sitio demuestra una implementación excelente en cuanto a cifrado de datos y redirecciones seguras. No obstante, se concluye que el sitio presenta vulnerabilidades moderadas relacionadas con la gestión de cookies y cabeceras de respuesta, lo que podría comprometer la privacidad de los usuarios en escenarios específicos.

Resumen de Riesgos

0	3	6	3	51
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 47 dias
Cabeceras de Seguridad	60	FALLO	Solo 3/6 presentes. Faltan: X-Frame-Options, Ref...
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 — 60/100

Estado: FALLO

Solo 3/6 presentes. Faltan: X-Frame-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: mw-web.eqiad.main-545446dfb-gr49k — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: script-src 'unsafe-eval' blob: 'self' meta.wikimedia.org *.wikimedia.org *.wikip...
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=106384710; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://es.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
- BAJO **Meta generator**
  Expone: MediaWiki 1.47.0-wmf.2

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 (19466 bytes)
- INFO **Reglas robots.txt**
  290 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://es.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] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea embebido en frames externos, facilitando ataques de clickjacking.
[HIGH] Cookie GeoIP - HttpOnly: La falta de este atributo permite que la cookie sea accesible mediante scripts del lado del cliente, aumentando el riesgo de robo en ataques XSS.
[HIGH] Cookie NetworkProbeLimit - HttpOnly: Al no estar protegida, esta cookie es vulnerable al acceso no autorizado a través de document.cookie.
[MEDIUM] Referrer-Policy: No existe una política definida, lo que provoca que se envíe información sensible sobre la procedencia del tráfico a terceros.
[MEDIUM] Permissions-Policy: La falta de esta cabecera impide restringir el uso de APIs del navegador como la cámara o el micrófono.
[MEDIUM] Cookie WMF-Last-Access - SameSite: La ausencia de este atributo hace que la cookie sea susceptible a ataques de falsificación de petición en sitios cruzados o CSRF.
[MEDIUM] Cookie WMF-Last-Access-Global - SameSite: Falta el atributo de seguridad SameSite, permitiendo posibles vectores de ataque CSRF.
[MEDIUM] Cookie GeoIP - SameSite: Esta cookie carece de restricción de contexto, lo que facilita su explotación en peticiones cruzadas no deseadas.
[MEDIUM] Bloqueo total en robots.txt: El archivo bloquea la indexación de todo el sitio mediante la directiva Disallow: /, lo que afecta la visibilidad en buscadores.
[LOW] Server header expuesto: La cabecera revela información interna de la infraestructura mw-web.eqiad.main-545446dfb-gr49k.
[LOW] Meta generator: Se expone públicamente la versión exacta MediaWiki 1.47.0-wmf.2, lo cual facilita la búsqueda de exploits específicos.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a un directorio de administración, revelando rutas privadas a posibles atacantes.