

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://utileria.onrender.com/	Checks	9 pruebas
Dominio	utileria.onrender.com	Hallazgos	44 totales
Fecha	30 de septiembre de 2026 a las 00:19	Problemas	8 detectados

B

79/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada al sitio web utileria.onrender.com arroja una puntuacion de 79/100, lo que representa una nota B segun los estandares de evaluacion. Se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 genero una advertencia por puertos expuestos y 2 fallaron debido a la ausencia de cabeceras de seguridad y archivos de indexacion. Aunque el transporte de datos esta correctamente cifrado, la carencia de politicas de seguridad en las cabeceras HTTP expone a los usuarios a vectores de ataque conocidos. Se concluye que el sitio es parcialmente seguro, pero presenta vulnerabilidades moderadas que requieren atencion inmediata para fortalecer su postura defensiva.

Resumen de Riesgos

0	2	3	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 82 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 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	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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 82 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
82 dias restantes (expira: 2026-12-20T23:04:28.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-21T22:04:31.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Referrer-Policy, Permissions-Policy

- BAJO Server header expuesto
Server: cloudflare — 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=315360000; 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://utileria.onrender.com/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=315360000; includeSubdomains; preload
- BAJO

HSTS includeSubDomains
HSTS cubre subdominios
- INFO

HSTS max-age
max-age=315360000 (3650 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 — 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)
- BAJO

sitemap.xml
No encontrado (HTTP 404)
- BAJO

security.txt
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO

Puerto 8080 (HTTP-Alt)
ABIERTO — 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 ataques de Cross-Site Scripting (XSS) e inyeccion de contenido malicioso.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es vulnerable a ataques de clickjacking, permitiendo que atacantes carguen la web en frames invisibles.
[MEDIUM] Puerto 8080 (HTTP-Alt): Este puerto se encuentra abierto y suele ser utilizado para servicios de administracion o proxies, aumentando la superficie de ataque.

[MEDIUM] Referrer-Policy: La falta de esta política puede provocar la fuga de información sensible en las URLs de referencia hacia sitios externos.

[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs del navegador, lo que podría permitir el uso no autorizado de periféricos o geolocalización.

[LOW] Server header expuesto: Se detectó la cabecera Server: cloudflare, lo cual facilita a un atacante identificar la infraestructura subyacente.

[LOW] robots.txt: La ausencia de este archivo impide controlar que partes del sitio deben o no ser rastreadas por motores de búsqueda.

[LOW] sitemap.xml: No se encontró el mapa del sitio, lo que dificulta la indexación correcta y la auditoría de endpoints públicos.