EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://benevolent-scone-cf9566.netlify.app	Checks	9 pruebas
Dominio	benevolent-scone-cf9566.netlify.app	Hallazgos	44 totales
Fecha	12 de junio de 2026 a las 08:30	Problemas	8 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado sobre el sitio web ha arrojado una puntuacion de 80/100, lo que equivale a una calificacion de grado B. Se ejecutaron un total de 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 presentaron fallos criticos relacionados con la configuracion de cabeceras de seguridad y archivos de indexacion. No se detectaron vulnerabilidades en el transporte de datos ni en la gestion de cookies, manteniendo un estandar de cifrado optimo. Sin embargo, la ausencia de politicas de seguridad en el servidor permite concluir que el sitio es vulnerable a ataques de inyeccion y suplantacion de identidad. Se recomienda una intervencion tecnica para corregir las omisiones detectadas en la configuracion del servidor.

Resumen de Riesgos

0	2	3	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 281 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	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 — 100/100

Estado: OK

Certificado valido, expira en 281 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  281 dias restantes (expira: 2027-03-19T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-16T00:00:00.000Z
- 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: Netlify — 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=31536000; 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://benevolent-scone-cf9566.netlify.app/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 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 — 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 facilita ataques de Cross-Site Scripting (XSS) y la inyeccion de contenido no autorizado en el navegador del usuario.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking, permitiendo que atacantes carguen la web en marcos invisibles para engañar a los visitantes.

[MEDIUM] X-Content-Type-Options: La falta de esta proteccion permite el MIME-type sniffing, lo que podria obligar al navegador a interpretar archivos de forma distinta a la declarada, facilitando la ejecucion de codigo malicioso.
[MEDIUM] Referrer-Policy: No existe un control sobre la informacion de procedencia enviada en las peticiones salientes, lo que podria exponer rutas internas o datos sensibles de la navegacion.
[MEDIUM] Permissions-Policy: La falta de esta cabecera implica que no hay restricciones sobre el uso de APIs del navegador, como la camara o el microfono, por parte de scripts de terceros.
[LOW] Server header expuesto: El encabezado revela explicitamente el uso de la tecnologia Netlify, proporcionando informacion valiosa a posibles atacantes sobre la infraestructura del servidor.
[LOW] robots.txt: La inexistencia de este archivo genera un error 404 e impide gestionar correctamente el comportamiento de los rastreadores de motores de busqueda.
[LOW] sitemap.xml: El mapa del sitio no ha sido localizado, lo que afecta negativamente a la estructura de indexacion y visibilidad controlada del contenido web.