EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://aiautomatia.netlify.app/#	Checks	9 pruebas
Dominio	aiautomatia.netlify.app	Hallazgos	44 totales
Fecha	10 de mayo de 2026 a las 13:51	Problemas	8 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web ha arrojado una puntuación de 80/100, obteniendo una calificación de grado B. Se ejecutaron 9 comprobaciones pasivas, resultando en 7 evaluaciones satisfactorias y 2 fallos críticos relacionados con la configuración de cabeceras y archivos de servicio. El sitio presenta una base sólida en cuanto a cifrado de datos y transporte seguro, pero carece de políticas de protección contra ataques de inyección y suplantación. Se concluye que el sitio es moderadamente seguro, aunque vulnerable a vectores de ataque conocidos que podrían comprometer la integridad de la sesión del usuario.

Resumen de Riesgos

CRITICO	ALTO	MEDIO	BAJO	INFO
0	2	3	3	36

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 313 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 313 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  313 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://aiautomatia.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 permite la ejecución de scripts no autorizados, facilitando ataques de Cross-Site Scripting (XSS) e inyección de datos.
[HIGH] X-Frame-Options: Al no estar presente, el sitio puede ser cargado dentro de un iframe de un dominio malicioso, lo que facilita ataques de clickjacking para engañar al usuario.

[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite que los navegadores realicen MIME-type sniffing, pudiendo ejecutar archivos con contenido malicioso disfrazados de otros tipos.
[MEDIUM] Referrer-Policy: No se controla qué información de navegación se envía a otros sitios web, lo que podría derivar en la fuga de datos técnicos o de sesión a terceros.
[MEDIUM] Permissions-Policy: No se restringe el acceso de las APIs del navegador a funciones sensibles como la cámara o el micrófono, aumentando la superficie de ataque para scripts maliciosos.
[LOW] Server header expuesto: La cabecera revela el uso de Server: Netlify, proporcionando información valiosa a un atacante sobre la infraestructura tecnológica utilizada.
[LOW] robots.txt no encontrado: La falta de este archivo impide dar instrucciones claras a los rastreadores sobre qué partes del sitio deben o no ser indexadas.
[LOW] sitemap.xml no encontrado: La ausencia de un mapa del sitio dificulta la correcta gestión del contenido rastreable y la auditoría de endpoints expuestos.