EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://geintrab.ddns.net	Checks	9 pruebas
Dominio	geintrab.ddns.net	Hallazgos	49 totales
Fecha	26 de mayo de 2026 a las 13:15	Problemas	11 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha resultado en una puntuación de 70/100, lo que equivale a una calificación de nota C. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias y 1 fue calificado como fallo de seguridad. A pesar de contar con un cifrado de transporte válido, la ausencia total de cabeceras de protección y la configuración inadecuada de las cookies representan un riesgo significativo. En su estado actual, el sitio se considera vulnerable ante ataques de inyección de código y secuestro de sesiones. Es imperativo aplicar medidas correctivas en la configuración del servidor para elevar los estándares de protección.

Resumen de Riesgos

0	6	3	2	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 82 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	XSRF-TOKEN: falta HttpOnly; laravel_session: fal...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

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: 2026-08-16T10:21:41.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-18T10:21:42.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx/1.18.0 (Ubuntu) — 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
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://geintrab.ddns.net/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- 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

XSRF-TOKEN: falta HttpOnly; laravel_session: falta Secure

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: laravel_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: laravel_session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: laravel_session — SameSite**
  SameSite=lax

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (24 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- 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

[ALTA] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques de inyección de contenido y scripts maliciosos (XSS).
[ALTA] X-Frame-Options: Al no estar configurada, el sitio permite ser cargado en marcos externos, facilitando ataques de clickjacking.
[ALTA] Strict-Transport-Security: La falta de la directiva HSTS impide que el navegador obligue siempre el uso de conexiones cifradas, permitiendo ataques de degradación de protocolo.
[ALTA] Cookie XSRF-TOKEN: Carece del atributo HttpOnly, permitiendo que el token sea accesible mediante scripts y aumentando el riesgo de robo de identidad.
[ALTA] Cookie laravel_session: No implementa el flag Secure, lo que significa que los datos de sesión podrían transmitirse a través de conexiones HTTP no cifradas.
[MEDIA] X-Content-Type-Options: La falta de esta cabecera permite que los navegadores intenten adivinar el tipo de contenido, abriendo la puerta a ataques de sniffing de MIME.
[MEDIA] Referrer-Policy: No se ha definido una política de referencia, lo que provoca la fuga de información sensible en los encabezados de las peticiones salientes.
[MEDIA] Permissions-Policy: No se restringen las funcionalidades del navegador como la cámara o el micrófono, dejando expuestas APIs sensibles.
[BAJA] Server header expuesto: Se revela la tecnología específica nginx/1.18.0 (Ubuntu), lo que ayuda a posibles atacantes a buscar exploits conocidos para esa versión.
[BAJA] sitemap.xml: El archivo de mapa del sitio no fue encontrado, lo que dificulta la indexación correcta y el análisis de la estructura web.