

Escanear Vulnerabilidades

Informe de Seguridad Web

URL	https://illa-git-develop-delestalmiguelignacio-5787s-projects.vercel.app/	Checks	9 pruebas
Dominio	illa-git-develop-delestalmiguelignacio-5787s-projects.vercel.app	Hallazgos	47 totales
Fecha	17 de abril de 2026 a las 00:17	Problemas	7 detectados

B

83/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha arrojado una puntuación de 83/100, obteniendo una nota final de B. Durante la evaluación, se ejecutaron un total de 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 presentaron fallos críticos relacionados con la configuración de cabeceras de seguridad y archivos de indexación. Los resultados indican que, si bien el transporte de datos y el cifrado son sólidos, el sitio carece de protecciones esenciales contra ataques de inyección de contenido y exposición de infraestructura. Debido a la ausencia de políticas de seguridad en las cabeceras HTTP, el sitio se considera parcialmente vulnerable en su capa de aplicación. Es imperativo corregir las deficiencias en las políticas de respuesta para alcanzar un nivel de seguridad óptimo.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 40 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	1 cookies, todas con flags correctos
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 40 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
40 dias restantes (expira: 2026-05-27T06:28:02.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-02-26T06:28:03.000Z
- 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-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
Server: Vercel — Revela tecnologia del servidor

- **ALTO** **Content-Security-Policy**
Falta — Previene XSS y ataques de inyeccion de contenido
- **INFO** **X-Frame-Options**
Presente: DENY
- **INFO** **Strict-Transport-Security**
Presente: max-age=63072000; 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 308 redirige a <https://illa-git-develop-delestalmiguelignacio-5787s-projects.vercel.app/>
- **INFO** **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=63072000; includeSubDomains; preload
- **BAJO** **HSTS includeSubDomains**
HSTS cubre subdominios
- **INFO** **HSTS max-age**
max-age=63072000 (730 dias)
- **INFO** **Respuesta HTTPS**
HTTPS responde con status 401

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

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
1 cookie(s) encontrada(s)
- INFO **Cookie: _vercel_sso_nonce — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: _vercel_sso_nonce — Secure**
Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _vercel_sso_nonce — 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
No encontrado (HTTP 401)
- BAJO **sitemap.xml**
No encontrado (HTTP 401)
- 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 y ataques de inyección de código (XSS) en el navegador del usuario.
- [MEDIUM] X-Content-Type-Options: Falta esta configuración, lo que permite que el navegador realice "MIME-type sniffing" y pueda ejecutar archivos con extensiones maliciosas.
- [MEDIUM] Referrer-Policy: No existe una política definida, lo que provoca que se pueda filtrar información sensible de las URLs en las solicitudes salientes hacia otros dominios.
- [MEDIUM] Permissions-Policy: La falta de esta cabecera impide restringir el uso de APIs del navegador, como la cámara, el micrófono o la geolocalización, aumentando riesgos de privacidad.
- [LOW] Server header expuesto: El servidor responde con la cabecera "Server: Vercel", revelando la tecnología de infraestructura utilizada y facilitando la búsqueda de vulnerabilidades específicas.
- [LOW] robots.txt no encontrado: El archivo de instrucciones para motores de búsqueda devolvió un error 401, lo que impide una gestión adecuada del rastreo e indexación.
- [LOW] sitemap.xml no encontrado: La ausencia de este mapa del sitio, que también devolvió un error 401, dificulta la correcta navegación de los indexadores automáticos.