

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://linxrest.web.app/?r=lili-dmoca	Checks	9 pruebas
Dominio	linxrest.web.app	Hallazgos	44 totales
Fecha	27 de septiembre de 2026 a las 20:02	Problemas	4 detectados

A

90/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio linxrest.web.app ha arrojado una puntuación de 90/100, lo que corresponde a una nota de A. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo 7 resultados satisfactorios, 1 advertencia relacionada con cabeceras de seguridad y 1 fallo en archivos de configuración de rastreo. El sitio web demuestra una implementación robusta de protocolos de cifrado y transporte seguro, aunque presenta carencias en protecciones contra ataques de interfaz. En conclusión, el sitio es seguro en sus fundamentos de comunicación, pero se considera vulnerable a ataques de clickjacking y falta de políticas de permisos del navegador.

Resumen de Riesgos

0	1	1	2	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 86 dias
Cabeceras de Seguridad	70	AVISO	4/6 presentes. Faltan: X-Frame-Options, Permissi...
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 86 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
86 dias restantes (expira: 2026-12-22T17:59:57.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-23T17:59:58.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 70/100

Estado: AVISO

4/6 presentes. Faltan: X-Frame-Options, Permissions-Policy

- INFO Content-Security-Policy
Presente: default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.tailwindcss.co...

- ALTO

X-Frame-Options
Falta — Protege contra clickjacking
- INFO

Strict-Transport-Security
Presente: max-age=31556926; includeSubDomains; preload
- INFO

X-Content-Type-Options
Presente: nosniff
- INFO

Referrer-Policy
Presente: strict-origin-when-cross-origin
- 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://linxrest.web.app/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=31556926; includeSubDomains; preload
- BAJO

HSTS includeSubDomains
HSTS cubre subdominios
- INFO

HSTS max-age
max-age=31556926 (365 días)
- 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
- INFO

Tecnologias detectadas
React, Next.js

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)
- INFO

security.txt
Presente en /.well-known/security.txt — Buena practica

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] X-Frame-Options: Falta esta cabecera de seguridad, lo cual es peligroso porque permite que el sitio sea cargado dentro de un iframe, facilitando ataques de clickjacking para engañar al usuario.
[MEDIUM] Permissions-Policy: La ausencia de esta cabecera impide restringir el uso de APIs del navegador como la cámara, el micrófono o la geolocalización, aumentando el riesgo de abuso de hardware por scripts maliciosos.

[LOW] robots.txt: No se encontró el archivo (HTTP 404), lo que genera una falta de control sobre cómo los motores de búsqueda rastrean e indexan el contenido del sitio.

[LOW] sitemap.xml: El archivo no está presente, lo que dificulta la indexación estructurada y la visibilidad de la jerarquía del sitio web.