EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://studyalejandrx-study-alejandrx15.vercel.app/	Checks	9 pruebas
Dominio	studyalejandrx-study-alejandrx15.vercel.app	Hallazgos	52 totales
Fecha	13 de agosto de 2026 a las 23:18	Problemas	7 detectados

A

90/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio web ha arrojado una puntuacion exacta de 90/100 con una nota final de A. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo como resultado 6 verificaciones exitosas, 2 advertencias y 1 fallo en la configuracion de archivos de indexacion. Aunque la base de cifrado y transporte de datos es solida, se detectaron deficiencias en la proteccion de cookies y exposicion de archivos informativos. En conclusion, el sitio se considera seguro pero vulnerable a ataques de secuestro de sesion debido a la falta de atributos de seguridad en las cookies. No se realizo un pentest activo en este ciclo de auditoria.

Resumen de Riesgos

0	3	3	1	45
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 44 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: Permissions-Policy
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	67	AVISO	_v-anonymous-id: falta HttpOnly; _v-anonymous-id...
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 44 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  44 dias restantes (expira: 2026-09-26T13:27:56.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-28T13:27:57.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: default-src 'self' vercel.com *.vercel.com *.vercel.sh vercel.live *.stripe.com ...
- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: 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 308 redirige a https://studyalejandrx-study-alejandrx15.vercel.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
- INFO **Tecnologias detectadas**
  React, Next.js, Nuxt

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 67/100

Estado: AVISO

_v-anonymous-id: falta HttpOnly; _v-anonymous-id-renewed: falta HttpOnly; _v-consent: falta HttpOnly

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- ALTO **Cookie: _v-anonymous-id — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: _v-anonymous-id — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _v-anonymous-id — SameSite**
  SameSite=lax
- ALTO **Cookie: _v-anonymous-id-renewed — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: _v-anonymous-id-renewed — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _v-anonymous-id-renewed — SameSite**
  SameSite=lax
- ALTO **Cookie: _v-consent — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: _v-consent — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _v-consent — 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

- 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] Cookie _v-anonymous-id: Falta el atributo HttpOnly, permitiendo que la cookie sea accesible via scripts de cliente, aumentando el riesgo de ataques XSS.
[HIGH] Cookie _v-anonymous-id-renewed: Ausencia de flag HttpOnly que expone identificadores de usuario a posibles robos de sesion.
[HIGH] Cookie _v-consent: No tiene habilitado el atributo HttpOnly, lo que compromete la integridad de las preferencias de privacidad ante scripts maliciosos.
[MEDIUM] Permissions-Policy: Esta cabecera de seguridad no esta presente, impidiendo la restriccion de uso de APIs sensibles como la camara o el microfono.
[MEDIUM] Archivo /readme.html: El archivo es accesible publicamente y puede revelar informacion sobre la estructura o versiones del proyecto.
[MEDIUM] Archivo /README.txt: Documento expuesto que facilita a un atacante la recoleccion de datos sobre el despliegue del sitio.
[LOW] Cabecera Server expuesta: El valor Vercel es visible, revelando la tecnologia subyacente y facilitando el reconocimiento para ataques dirigidos.
[LOW] Ausencia de robots.txt y sitemap.xml: El sitio no cuenta con archivos de guia para rastreadores, lo que afecta el control de indexacion y SEO.