EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sales-dashboardd.replit.app/	Checks	9 pruebas
Dominio	sales-dashboardd.replit.app	Hallazgos	50 totales
Fecha	24 de marzo de 2026 a las 16:51	Problemas	15 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web muestra una puntuación de 70/100 con una nota de calificación C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando 6 de ellos satisfactorios y 3 con fallos de configuración críticos. El análisis revela que, aunque el sitio posee una base de cifrado adecuada, carece de las protecciones modernas necesarias para mitigar ataques de inyección y secuestro de sesiones. Debido a la ausencia de cabeceras de seguridad esenciales y el manejo inseguro de cookies, el sitio se clasifica actualmente como vulnerable ante amenazas comunes del entorno web. Se requiere una intervención inmediata para elevar los estándares de protección de la plataforma.

Resumen de Riesgos

0	4	9	2	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 85 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	0	FALLO	GAESA: falta HttpOnly; GAESA: falta Secure; GAES...
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 85 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  85 dias restantes (expira: 2026-06-18T00:20:46.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-19T23:24:51.000Z
- 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: Google Frontend — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Express — Revela framework/lenguaje
- 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=63072000; includeSubDomains
- 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://sales-dashboardd.replit.app:443/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 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**
  Express

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
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 0/100

Estado: FALLO

GAESA: falta HttpOnly; GAESA: falta Secure; GAESA: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: GAESA — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: GAESA — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: GAESA — SameSite**
  Falta SameSite — Vulnerable a CSRF

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] Falta de Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso.
[HIGH] Falta de X-Frame-Options: Al no estar definida, el sitio es susceptible a ataques de clickjacking, permitiendo que sea embebido en marcos externos no autorizados.
[HIGH] Cookie GAESA sin flag HttpOnly: La cookie es accesible mediante scripts del lado del cliente, lo que aumenta significativamente el riesgo de robo de sesión.
[HIGH] Cookie GAESA sin flag Secure: El identificador de sesión puede ser transmitido a través de canales no cifrados, exponiéndolo a intercepción en redes abiertas.
[MEDIUM] Falta de X-Content-Type-Options: El navegador puede intentar interpretar el tipo de archivo de forma incorrecta, lo que podría derivar en la ejecución de código no deseado.
[MEDIUM] Falta de Referrer-Policy: No existe control sobre la información que el navegador envía a otros sitios al seguir enlaces, comprometiendo la privacidad de los usuarios.
[MEDIUM] Falta de Permissions-Policy: No se restringe el acceso de la aplicación a funciones del hardware o APIs del navegador como la cámara o geolocalización.
[MEDIUM] Cookie GAESA sin flag SameSite: La falta de este atributo hace que el sitio sea vulnerable a ataques de falsificación de solicitudes entre sitios (CSRF).
[MEDIUM] Rutas de administración y archivos informativos expuestos: Se detectó acceso público a paneles como /wp-login.php, /administrator/ y archivos README que revelan detalles técnicos.
[LOW] Exposición de cabecera Server: Se revela el uso de Google Frontend, proporcionando información técnica que ayuda a un atacante a perfilar el servidor.
[LOW] Exposición de cabecera X-Powered-By: El sitio confirma el uso del framework Express, limitando el anonimato tecnológico de la infraestructura.
[LOW] Ausencia de archivos robots.txt y sitemap.xml: La falta de estos archivos dificulta la indexación controlada y no sigue las mejores prácticas de configuración web.