

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://movilprofit.com
Dominio movilprofit.com
Fecha 22 de junio de 2026 a las 13:07

Checks 9 pruebas
Hallazgos 42 totales
Problemas 12 detectados

C

68/100

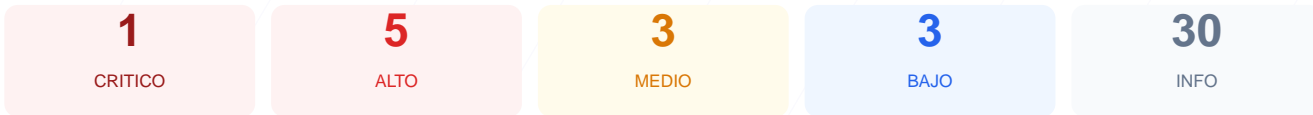
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el sitio web arroja una puntuación de 68/100, lo que otorga una calificación de grado C. Se completaron exitosamente 9 checks pasivos, resultando en 5 verificaciones correctas, 2 advertencias y 2 fallos críticos en la configuración. Aunque el cifrado de transporte inicial es adecuado, la infraestructura presenta debilidades significativas en la protección de cabeceras y exposición de servicios. En conclusión, el sitio se considera vulnerable debido a la exposición de puertos críticos de bases de datos y la ausencia total de políticas de seguridad en el navegador.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 72 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	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	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 72 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
72 dias restantes (expira: 2026-09-02T06:49:40.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-06-04T06:49:41.000Z
- 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: Apache — 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://movilprofit.com/>
- **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 — 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)
- BAJO **security.txt**
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- ALTO **Puerto 21 (FTP)**
ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
ABIERTO — 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 autentificacion 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

[CRITICAL] Puerto 3306 (MySQL): Servicio de base de datos expuesto públicamente, permitiendo intentos de acceso externo o ataques de fuerza bruta.

[HIGH] Puerto 21 (FTP): Protocolo de transferencia de archivos sin cifrar abierto, lo que facilita la interceptación de credenciales en la red.

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).

[HIGH] X-Frame-Options: La falta de esta directiva hace que el sitio sea susceptible a ataques de clickjacking mediante el uso de marcos externos.

[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide que el navegador fuerce automáticamente conexiones seguras HTTPS.

[MEDIUM] X-Content-Type-Options: El servidor no previene el sniffing de tipos MIME, lo que podría permitir que archivos maliciosos sean interpretados como scripts.

[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada a terceros, comprometiendo potencialmente la privacidad de la navegación.

[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la geolocalización.

[LOW] Server header expuesto: El encabezado revela el uso de Apache, proporcionando información técnica valiosa para que un atacante busque exploits específicos.

[LOW] Archivos de rastreo faltantes: La inexistencia de robots.txt y sitemap.xml dificulta la gestión adecuada del indexado y la auditoría de rutas del sitio.