EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://miprofit.com	Checks	9 pruebas
Dominio	miprofit.com	Hallazgos	48 totales
Fecha	22 de junio de 2026 a las 13:11	Problemas	18 detectados

D

50/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web miprofit.com arroja una puntuación de 50/100, lo que corresponde a una calificación de grado D. El análisis se basó en la ejecución de 9 comprobaciones pasivas, de las cuales 3 resultaron exitosas, 2 generaron advertencias y 4 fallaron de manera crítica. Se han detectado deficiencias graves en la configuración de cabeceras de seguridad y una exposición peligrosa de servicios de infraestructura en puertos abiertos. Debido a estos hallazgos, el sitio se considera actualmente vulnerable y presenta una superficie de ataque considerable para actores malintencionados.

Resumen de Riesgos

1	6	8	3	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 35 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	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 1 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	4 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 35 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  35 dias restantes (expira: 2026-07-27T15:33:49.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-07-28T15:45:48.000Z
- 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: LiteSpeed — 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://miprofit.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

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Site Kit by Google 1.181.0
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 1 expuesta

- ALTO **WordPress version**
  Version 1 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)

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 — 20/100

Estado: FALLO

4 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://34.197.85.152/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://mundoprofit.com
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://34.197.85.152/
- MEDIO **href (link/stylesheet)**
  ...y 1 mas del mismo tipo

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (29 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 0 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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 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

[CRITICAL] Puerto 3306 (MySQL): El puerto de la base de datos está abierto al público, lo que permite intentos de acceso no autorizados y ataques de fuerza bruta.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques de Cross-Site Scripting (XSS) e inyección de contenido.
[HIGH] X-Frame-Options: Falta de configuración que protege el sitio contra ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se ha implementado HSTS, impidiendo que el navegador fuerce siempre conexiones seguras a través de HTTPS.
[HIGH] WordPress versión: La versión 1 del CMS se expone públicamente, permitiendo a los atacantes identificar y explotar vulnerabilidades conocidas (CVEs).
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos sin cifrado abierto, lo que expone credenciales y datos en tránsito.
[MEDIUM] X-Content-Type-Options: Falta de cabecera para prevenir que el navegador interprete archivos con tipos MIME incorrectos (sniffing).
[MEDIUM] Referrer-Policy: Ausencia de control sobre la información de procedencia que se envía al navegar hacia otros sitios.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, dejando activos permisos potenciales para cámara, micrófono o geolocalización.
[MEDIUM] Contenido Mixto: Se detectaron 4 recursos cargados mediante HTTP inseguro, incluyendo referencias a la IP 34.197.85.152 y al dominio mundoprofit.com.
[MEDIUM] Puerto 22 (SSH): El acceso remoto por terminal está expuesto, aumentando el riesgo de ataques dirigidos al servidor.
[LOW] Server header: El servidor revela el uso de tecnología LiteSpeed, proporcionando información útil para el perfilado de ataques.
[LOW] Meta generator: La etiqueta meta expone el uso de Site Kit by Google 1.181.0.
[LOW] sitemap.xml: El archivo de mapa del sitio no fue encontrado, lo que afecta la auditoría de la estructura web.