EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://tiendanegocio.com/	Checks	9 pruebas
Dominio	tiendanegocio.com	Hallazgos	51 totales
Fecha	7 de mayo de 2026 a las 13:52	Problemas	14 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado a tiendanegocio.com arroja una puntuación de 65/100, lo que equivale a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 5 verificaciones correctas, 2 advertencias y 2 fallos críticos de configuración. Aunque el sitio cuenta con un cifrado de transporte válido, la ausencia total de cabeceras de seguridad y deficiencias en el manejo de cookies comprometen la integridad de la plataforma. En su estado actual, el sitio se considera vulnerable ante ataques de intermediarios, inyección de contenido y secuestro de sesiones.

Resumen de Riesgos

0	6	6	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 59 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	33	FALLO	abVersion: falta Secure; abVersion: falta SameSi...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 59 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  59 dias restantes (expira: 2026-07-05T21:43:21.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-06T21:43:22.000Z
- 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/2.4.41 (Ubuntu) — 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
- 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://tiendanegocio.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
- INFO **Tecnologias detectadas**
  Next.js, Express

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 — 33/100

Estado: FALLO

abVersion: falta Secure; abVersion: falta SameSite; abVersion: falta Secure; abVersion: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: abVersion — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: abVersion — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: abVersion — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: abVersion — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: abVersion — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: abVersion — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://qr.afip.gob.ar/?qr=ZvIj0pNHDXEtXyw70xmlig,,

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (139 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://tiendanegocio.com/robots.txtqaweq
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de Cross-Site Scripting (XSS) y diversos métodos de inyección de contenido malicioso.
[HIGH] X-Frame-Options: La ausencia de esta política permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No existe configuración HSTS, lo que impide que el navegador obligue el uso de conexiones seguras HTTPS permanentemente.
[HIGH] Cookies sin flag Secure: La cookie abVersion carece del flag Secure, permitiendo que la información se transmita a través de conexiones HTTP no cifradas.
[MEDIUM] Cookies sin atributo SameSite: La cookie abVersion no tiene configurado el atributo SameSite, dejando a los usuarios vulnerables a ataques de Cross-Site Request Forgery (CSRF).
[MEDIUM] Contenido Mixto: Se detectó un recurso de hoja de estilo externo vinculado a AFIP cargando mediante HTTP, lo que degrada la seguridad de la página HTTPS.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador realice MIME-type sniffing, pudiendo ejecutar archivos con extensiones incorrectas de forma maliciosa.
[MEDIUM] Referrer-Policy y Permissions-Policy: El sitio no controla qué información de navegación se comparte con terceros ni restringe el acceso a APIs sensibles del navegador.
[LOW] Cabecera Server expuesta: El servidor revela Apache/2.4.41 (Ubuntu), proporcionando información técnica específica que facilita la búsqueda de exploits conocidos.
[LOW] Cabecera X-Powered-By expuesta: Se detectó el valor Express, informando a posibles atacantes sobre el framework de desarrollo utilizado.