EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://teamit.com.co	Checks	9 pruebas
Dominio	teamit.com.co	Hallazgos	39 totales
Fecha	23 de abril de 2026 a las 15:58	Problemas	9 detectados

B

75/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web arroja una puntuación de 75/100 con una calificación de nota B. El análisis se fundamentó en la ejecución de 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 2 presentaron fallos críticos relacionados con la configuración de seguridad. Si bien la integridad de la conexión está garantizada por un certificado SSL válido, existen carencias importantes en las políticas de protección del navegador. Se concluye que el sitio es moderadamente seguro, pero presenta vulnerabilidades de configuración que podrían ser explotadas por atacantes para realizar inyecciones de código. El estado general requiere atención en las capas de cabeceras HTTP y visibilidad de archivos internos.

Resumen de Riesgos

0	2	5	2	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 331 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
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	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 331 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  331 dias restantes (expira: 2027-03-20T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-27T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Microsoft-IIS/10.0 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- 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.)

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**
  ASP.NET

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 — 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 **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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: La ausencia de esta cabecera permite la ejecución de scripts no autorizados, aumentando el riesgo de ataques XSS.
[HIGH] Strict-Transport-Security: No se aplica la política HSTS, lo que impide forzar de forma estricta las conexiones seguras mediante HTTPS.
[MEDIUM] X-Content-Type-Options: Al faltar esta cabecera, el sitio es vulnerable a ataques de MIME-type sniffing para ejecutar archivos maliciosos.
[MEDIUM] Referrer-Policy: La falta de control sobre la información de referencia puede exponer datos de navegación a dominios externos.
[MEDIUM] Permissions-Policy: No se restringe el acceso de las APIs del navegador a componentes del hardware del usuario.
[MEDIUM] Archivos informativos expuestos: El acceso público a /readme.html y /README.txt puede revelar detalles técnicos sensibles sobre la plataforma.
[LOW] Server header expuesto: La cabecera Server revela el uso de Microsoft-IIS/10.0, facilitando el reconocimiento para ataques dirigidos.
[LOW] X-Powered-By expuesto: Se revela que el sitio utiliza el framework ASP.NET, lo que reduce el esfuerzo de un atacante para identificar vectores específicos.