EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://middleman.stmplus.cloud/	Checks	9 pruebas
Dominio	middleman.stmplus.cloud	Hallazgos	46 totales
Fecha	12 de mayo de 2026 a las 01:47	Problemas	10 detectados

C

67/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web analizado ha obtenido una puntuación de 67/100, lo que le otorga una calificación de nota C. Este resultado se deriva de la ejecución de 9 checks pasivos, de los cuales 5 fueron satisfactorios, 2 generaron advertencias y 2 resultaron en fallos de seguridad. Se han identificado carencias importantes en la implementación de cabeceras de protección y en la redirección obligatoria de tráfico cifrado. Debido a estos hallazgos, se concluye que el sitio es actualmente vulnerable ante ataques de interceptación de datos y manipulación de contenido.

Resumen de Riesgos

0	4	3	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 64 dias
Cabeceras de Seguridad	40	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a 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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 64 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  64 dias restantes (expira: 2026-07-15T05:34:06.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-16T05:34:07.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 40/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Next.js — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: DENY
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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**
  React, Next.js, Next.js

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1738 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — 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) e inyección de código.
[HIGH] Falta de Strict-Transport-Security: Al no existir esta directiva, no se obliga al navegador a utilizar siempre conexiones HTTPS, permitiendo ataques de degradación de SSL.
[HIGH] Fallo en redirección HTTPS: El servidor responde con éxito en el puerto 80 (HTTP) sin redirigir al puerto seguro, exponiendo la comunicación a ser escuchada por terceros.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de este puerto expuesto aumenta la superficie de ataque al ofrecer un servicio web alternativo potencialmente menos vigilado.
[MEDIUM] Falta de Permissions-Policy: El sitio no restringe el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[MEDIUM] Bloqueo total en robots.txt: El archivo impide el indexado de todo el contenido, lo cual es inusual en sitios de producción y puede ocultar rutas críticas.
[LOW] Server header expuesto: El servidor revela que utiliza la infraestructura de Cloudflare, lo que ayuda a posibles atacantes a perfilar el objetivo.
[LOW] X-Powered-By expuesto: Se detectó el uso de Next.js, revelando el framework tecnológico y facilitando la búsqueda de exploits específicos para esa versión.
[LOW] Falta de sitemap.xml: La ausencia de este archivo dificulta la auditoría de la estructura del sitio y la correcta organización de sus endpoints.