EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://api23go.coop23dejulio.fin.ec	Checks	9 pruebas
Dominio	api23go.coop23dejulio.fin.ec	Hallazgos	39 totales
Fecha	27 de abril de 2026 a las 14:13	Problemas	3 detectados

A

95/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado en la infraestructura de api23go.coop23dejulio.fin.ec arroja una puntuación de 95/100 con una nota final de A. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 7 resultaron exitosos y se registró un fallo técnico en la configuración de archivos de control. La plataforma demuestra una implementación robusta en cuanto a cifrado SSL/TLS y protección mediante cabeceras de seguridad. Se concluye que el sitio es seguro y presenta una postura defensiva sólida, requiriendo únicamente ajustes menores para optimizar su configuración externa.

Resumen de Riesgos

0	0	0	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 128 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 128 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  128 dias restantes (expira: 2026-09-02T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-08-27T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

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

- INFO **Content-Security-Policy**
  Presente: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN, SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=15552000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff, nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer, strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(), microphone=(), camera=(), fullscreen=(self)

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 — 100/100

Estado: OK

1 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)**
  Cerrado — 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

[LOW] Server header expuesto: El servidor revela el uso de nginx, lo cual facilita el reconocimiento de tecnología por parte de posibles atacantes.
[LOW] Ausencia de archivo robots.txt: No se encontró el archivo en el servidor, impidiendo la gestión del rastreo por parte de bots y herramientas automáticas.
[LOW] Ausencia de sitemap.xml: La falta de este archivo dificulta la auditoría de la estructura del sitio y la indexación controlada.
[INFO] Redirección HTTPS no verificada: No se pudo confirmar que el tráfico inseguro se redirija automáticamente a la versión cifrada, lo que podría exponer datos en tránsito.