

Escanear Vulnerabilidades

Informe de Seguridad Web

URL	https://www.23virtual.coop23dejulio.fin.ec:9443/CWCREST/[URL_API]s	9 pruebas
Dominio	www.23virtual.coop23dejulio.fin.ec	Hallazgos 41 totales
Fecha	17 de abril de 2026 a las 22:25	Problemas 11 detectados

D

57/100

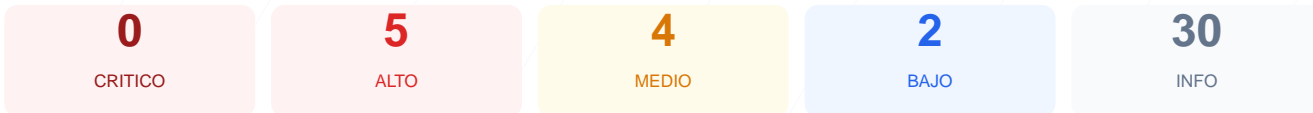
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado arroja una puntuación de 57/100, lo que resulta en una calificación técnica de grado D. Se completaron 9 verificaciones pasivas, identificando 5 puntos correctos, 1 advertencia por servicios expuestos y 3 fallos críticos en la configuración del servidor. A pesar de contar con un cifrado de transporte válido, la ausencia de protecciones contra ataques de inyección y la falta de redirección segura son debilidades latentes. Por lo tanto, se concluye que el sitio se encuentra en un estado vulnerable y requiere intervención inmediata para mitigar riesgos operativos.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 299 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 299 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
299 dias restantes (expira: 2027-02-10T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-02-04T00:00:00.000Z
- 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

- 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 — 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

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 — 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] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
- [HIGH] X-Frame-Options: Falta de protección que permite ataques de clickjacking, donde un tercero puede cargar el sitio en marcos invisibles para engañar al usuario.
- [HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide que el navegador establezca conexiones seguras de forma obligatoria y permanente.
- [HIGH] Redirección HTTP a HTTPS: El sistema permite conexiones no cifradas sin redirigirlas automáticamente, exponiendo la información en tránsito a posibles interceptaciones.
- [MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó un puerto de servidor web alternativo abierto que podría ser utilizado como vector de entrada para ataques dirigidos.
- [MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido, facilitando la ejecución de scripts maliciosos disfrazados.
- [MEDIUM] Referrer-Policy: No existe control sobre la información que el navegador envía a otros dominios al navegar desde este sitio.
- [MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente el acceso no autorizado a funciones como la cámara o el micrófono.

[LOW] Ausencia de robots.txt: No se encontraron instrucciones para rastreadores, lo que puede exponer directorios sensibles a motores de búsqueda.

[LOW] Ausencia de sitemap.xml: El sitio carece de un mapa estructurado, dificultando la auditoría de rutas y la indexación correcta de sus recursos.