EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://roifive.com	Checks	9 pruebas
Dominio	roifive.com	Hallazgos	44 totales
Fecha	22 de mayo de 2026 a las 14:20	Problemas	7 detectados

B

75/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web ha arrojado una puntuación de 75/100 con una calificación final de grado B. Se ejecutaron 9 comprobaciones pasivas, resultando en 5 verificaciones satisfactorias, 3 advertencias y 1 fallo crítico relacionado con el transporte de datos. Aunque el cifrado SSL es correcto, la ausencia de mecanismos de redirección obligatoria compromete la integridad de las conexiones. En su estado actual, el sitio se considera parcialmente vulnerable debido a configuraciones de red y cabeceras de seguridad incompletas que podrían ser explotadas.

Resumen de Riesgos

0	3	2	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 47 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
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 47 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  47 dias restantes (expira: 2026-07-08T22:34:01.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-09T22:34:02.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

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

- INFO **Content-Security-Policy**
  Presente: default-src 'none'; script-src 'nonce-oVXx0S8wV0hT2AnMsB86gw' 'unsafe-eval' http...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: same-origin
- INFO **Permissions-Policy**
  Presente: accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-write=...

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 403 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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 — 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 403)
- 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

[ALTA] HTTP a HTTPS redireccion: El servidor devuelve un error 403 en lugar de redirigir el tráfico inseguro a la versión cifrada del sitio.
[ALTA] HSTS (Strict-Transport-Security): La cabecera HSTS no está configurada, lo que impide que los navegadores fuercen conexiones seguras automáticamente.
[MEDIA] Puerto 8080 (HTTP-Alt) ABIERTO: La presencia de un puerto alternativo accesible aumenta la superficie de ataque y expone servicios potencialmente vulnerables.

[MEDIA] Bloqueo total en robots.txt: El archivo bloquea la indexación de todo el contenido, lo cual puede ser un indicativo de configuraciones de acceso mal gestionadas.
[BAJA] Server header expuesto: Se revela el uso de Cloudflare como tecnología de servidor, facilitando la fase de reconocimiento para un atacante.
[BAJA] sitemap.xml no encontrado: El archivo de mapa del sitio no está disponible, dificultando la validación de la estructura del dominio.