EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://m3s.com.ar/liga/	Checks	9 pruebas
Dominio	m3s.com.ar	Hallazgos	46 totales
Fecha	3 de junio de 2026 a las 19:31	Problemas	13 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio m3s.com.ar/liga ha dado como resultado una puntuación de 59/100, lo que equivale a una calificación de grado D. Durante la auditoría se ejecutaron 9 comprobaciones pasivas, de las cuales 5 resultaron satisfactorias, 2 generaron advertencias y 2 presentaron fallos críticos. El sitio web muestra una carencia total de cabeceras de seguridad esenciales y no implementa una redirección obligatoria hacia tráfico cifrado. En su estado actual, se concluye que el sitio es vulnerable ante ataques de interceptación de datos y ataques de inyección debido a una configuración de servidor incompleta.

Resumen de Riesgos

0	5	5	3	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 71 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	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 71 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  71 dias restantes (expira: 2026-08-13T22:19:58.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-15T21:21:20.000Z
- 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

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: CyberPanel-OLS/2.4.4 — Revela framework/lenguaje
- 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
- INFO **Tecnologias detectadas**
  CyberPanel-OLS/2.4.4

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] Ausencia de redirección HTTP a HTTPS: El sitio permite conexiones no cifradas, lo que facilita la interceptación de tráfico y datos sensibles.
[HIGH] Content-Security-Policy ausente: La falta de esta cabecera expone el sitio a ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options ausente: Esta omisión permite que el sitio sea cargado dentro de marcos de otras webs, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security ausente: El servidor no instruye a los navegadores para que utilicen exclusivamente conexiones seguras mediante HSTS.
[MEDIUM] X-Content-Type-Options ausente: Permite que el navegador realice MIME-sniffing, lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy ausente: No se controla la cantidad de información que el navegador envía al navegar desde este sitio hacia otros enlaces.
[MEDIUM] Permissions-Policy ausente: El sitio no restringe el acceso de las APIs del navegador a funciones sensibles como la cámara, el micrófono o la ubicación.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de puertos alternativos aumenta la superficie de ataque y suele estar vinculada a servicios administrativos mal configurados.
[MEDIUM] Bloqueo total en robots.txt: El archivo robots.txt bloquea todo el contenido del sitio, lo cual puede interferir con la visibilidad y auditoría de recursos.
[LOW] Cabecera Server expuesta: Se revela el uso de Cloudflare, proporcionando información técnica que puede ser aprovechada en la fase de reconocimiento de un ataque.
[LOW] X-Powered-By expuesto: El servidor indica explícitamente el uso de CyberPanel-OLS/2.4.4, permitiendo a un atacante buscar vulnerabilidades específicas para ese framework.
[LOW] Sitemap.xml no encontrado: La ausencia de este archivo dificulta la indexación estructurada y el análisis de la jerarquía del sitio.