EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://servicios.sanlorenzo.gov.ar	Checks	9 pruebas
Dominio	servicios.sanlorenzo.gov.ar	Hallazgos	15 totales
Fecha	30 de julio de 2026 a las 03:11	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web servicios.sanlorenzo.gov.ar arroja una puntuación de 73/100, lo que corresponde a una nota C. Durante la auditoría se ejecutaron 9 checks pasivos, resultando en 1 verificación exitosa, 0 advertencias y 1 fallo crítico relacionado con la infraestructura de indexación. Debido a la imposibilidad de validar protocolos de cifrado y cabeceras de seguridad esenciales, el sitio presenta una postura defensiva debilitada. En conclusión, el portal se considera vulnerable ya que no se puede garantizar la integridad y privacidad de las conexiones de los usuarios en su estado actual.

Resumen de Riesgos

1	0	0	2	12
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
  No se pudo establecer conexion SSL/TLS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  Error al acceder
- BAJO **sitemap.xml**
  Error al acceder

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — 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

[CRITICAL] Conexion SSL/TLS: No se pudo establecer una conexion segura con el servidor, lo que impide el cifrado de la informacion y facilita ataques de interceptacion de datos.
[HIGH] Cabeceras de Seguridad: No se detectaron encabezados de proteccion HTTP, dejando el sitio expuesto a ataques de inyeccion, clickjacking y ejecucion de scripts maliciosos.
[HIGH] Redireccion HTTPS: El servidor no garantiza el salto automatico de trafico inseguro a seguro, permitiendo que los usuarios naveguen por canales no cifrados.
[MEDIUM] Seguridad de Cookies: No se pudo verificar la presencia de atributos de seguridad en las cookies, lo que podria permitir el robo de sesiones de usuario.
[LOW] Ausencia de robots.txt y sitemap.xml: El sitio carece de archivos de directivas para buscadores, lo que afecta la organizacion del contenido y la eficiencia de la indexacion web.