EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Mendoza.gob.ar	Checks	9 pruebas
Dominio	mendoza.gob.ar	Hallazgos	15 totales
Fecha	18 de abril de 2026 a las 07:08	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar el análisis técnico del portal, se ha determinado una puntuación de 73/100, lo que corresponde a una calificación de grado C. El proceso consistió en la ejecución de nueve verificaciones pasivas, de las cuales una resultó exitosa y una presentó fallos directos de acceso, mientras que el resto no pudo ser validado por errores de respuesta del servidor. La imposibilidad de confirmar parámetros esenciales como el cifrado SSL y las cabeceras de protección sugiere una configuración que bloquea el reconocimiento externo o carece de optimización. Debido a estas incertidumbres técnicas, el sitio se considera vulnerable bajo el estándar de auditoría actual. Se requiere una intervención técnica para validar los componentes que no respondieron al escaneo.

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] Error de conexión SSL/TLS: No se pudo establecer una conexión segura con el servidor, impidiendo validar el cifrado de datos.
[HIGH] Cabeceras de seguridad no verificadas: La ausencia de respuesta en este control sugiere que el sitio carece de protecciones contra ataques de inyección y suplantación.
[MEDIUM] Seguridad de cookies no validada: No se pudo confirmar la presencia de atributos esenciales para prevenir el robo de sesiones de usuario.
[LOW] Ausencia de robots.txt: El archivo de directrices para rastreadores no es accesible, lo que afecta la gestión de la privacidad del sitio.
[LOW] Ausencia de sitemap.xml: No se localizó el mapa del sitio, dificultando la auditoría de rutas y la indexación correcta del contenido.
[MEDIUM] Redirección HTTPS no confirmada: No fue posible verificar si el tráfico inseguro se redirige automáticamente a una conexión cifrada.