EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://emco.mil.cl	Checks	9 pruebas
Dominio	emco.mil.cl	Hallazgos	15 totales
Fecha	24 de marzo de 2026 a las 21:36	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al dominio web arroja una puntuación de 73/100, lo que corresponde a una nota C según los estándares de auditoría. Se ejecutaron un total de 9 checks pasivos, de los cuales 1 resultó en estado OK, 0 presentaron advertencias y 1 fue clasificado como fallo crítico. La imposibilidad de verificar parámetros esenciales de cifrado y configuración de servidor sugiere una infraestructura web debilitada o mal configurada. En su estado actual, el sitio se considera vulnerable debido a la ausencia de validaciones de seguridad fundamentales.

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: No se pudo establecer una conexión segura SSL/TLS, lo que impide cifrar la comunicación entre el usuario y el servidor.
[CRITICAL] Cabeceras de Seguridad: Ausencia total de encabezados HTTP de protección, dejando el sitio expuesto a ataques de intermediario y ejecución de scripts maliciosos.
[CRITICAL] Redireccion HTTPS: El servidor no garantiza la transición automática hacia una conexión cifrada, permitiendo el acceso mediante protocolos inseguros.
[CRITICAL] Seguridad de Cookies: No se pudo validar la presencia de atributos de seguridad en las cookies, lo que facilita el robo de sesiones.
[LOW] Robots.txt y Sitemap: El acceso a estos archivos falló, lo que entorpece la correcta indexación y gestión del tráfico de rastreadores.