EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://bo-e-factura-pre.govern.ad/	Checks	9 pruebas
Dominio	bo-e-factura-pre.govern.ad	Hallazgos	15 totales
Fecha	16 de junio de 2026 a las 14:54	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web https://bo-e-factura-pre.govern.ad/ ha arrojado una puntuación de 73/100, lo que corresponde a una nota C. Durante la evaluación se ejecutaron un total de 9 checks pasivos, resultando en 1 verificación exitosa, 0 advertencias y 1 fallo crítico detectado. Los resultados muestran dificultades técnicas para validar componentes esenciales como el cifrado SSL y las cabeceras de seguridad. Debido a la incapacidad de confirmar protocolos básicos de protección de datos, se concluye que el sitio es actualmente vulnerable y requiere intervención técnica.

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 cifrada SSL/TLS, lo que impide asegurar la integridad y privacidad de la información transmitida.
[LOW] robots.txt: Se detectó un error al intentar acceder al archivo de directivas de indexación, lo que puede afectar el comportamiento de los motores de búsqueda.
[LOW] sitemap.xml: El mapa del sitio no está accesible o no existe, dificultando la navegación estructurada para sistemas automatizados.
[MEDIUM] Cabeceras de Seguridad: Error en la verificación de cabeceras, lo que implica una posible ausencia de protecciones contra ataques de clickjacking y XSS.
[MEDIUM] Seguridad de Cookies: No se pudo validar la configuración de cookies, aumentando el riesgo de secuestro de sesión si no poseen atributos Secure o HttpOnly.