EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://api-internal.erco.energy	Checks	9 pruebas
Dominio	api-internal.erco.energy	Hallazgos	19 totales
Fecha	23 de abril de 2026 a las 22:26	Problemas	12 detectados

F

10/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del dominio api-internal.erco.energy ha dado como resultado una puntuación de 10/100, lo que equivale a una nota de F. Durante la evaluación se ejecutaron 9 checks pasivos que revelaron fallos críticos, incluyendo la falta de un certificado SSL válido y la exposición masiva de servicios de infraestructura. El sistema no redirige el tráfico a conexiones seguras y presenta múltiples puertos de bases de datos abiertos directamente a internet. No se detectaron medidas de seguridad básicas activas, lo que compromete la integridad y confidencialidad de la información. En conclusión, el sitio es extremadamente vulnerable y requiere intervención inmediata para mitigar riesgos de intrusión.

Resumen de Riesgos

6	2	2	2	7
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
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	20	FALLO	8 puertos riesgosos abiertos

SSL/TLS — 0/100

Estado: FALLO

Certificado SSL no valido

- CRITICO **Certificado valido**
  El certificado SSL NO es valido
- INFO **Dias hasta expiracion**
  3399 dias restantes (expira: 2035-08-13T18:38:17.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-08-15T18:38:17.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS

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 — 20/100

Estado: FALLO

8 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — Acceso remoto seguro
- CRITICO **Puerto 23 (Telnet)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — Base de datos PostgreSQL expuesta
- CRITICO **Puerto 6379 (Redis)**
  ABIERTO — Cache Redis sin autenticacion por defecto
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- CRITICO **Puerto 27017 (MongoDB)**
  ABIERTO — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Certificado SSL no válido: El certificado actual no es de confianza, lo que impide establecer conexiones cifradas seguras entre el usuario y el servidor.
[CRITICAL] Puerto 23 (Telnet) ABIERTO: Servicio de acceso remoto que transmite toda la información, incluyendo credenciales, en texto plano sin cifrar.
[CRITICAL] Puerto 3306 (MySQL) ABIERTO: La base de datos MySQL es accesible desde internet, lo que permite ataques de fuerza bruta y posibles fugas de datos.
[CRITICAL] Puerto 5432 (PostgreSQL) ABIERTO: Exposición directa del servicio de base de datos PostgreSQL, aumentando el riesgo de acceso no autorizado a información estructurada.
[CRITICAL] Puerto 6379 (Redis) ABIERTO: El motor de caché está expuesto; estos servicios suelen carecer de contraseña por defecto, facilitando el robo de sesiones en memoria.
[CRITICAL] Puerto 27017 (MongoDB) ABIERTO: Base de datos NoSQL expuesta públicamente, lo que representa un riesgo máximo de exfiltración de documentos y datos sensibles.
[HIGH] HTTP a HTTPS redirección: El servidor permite conexiones por el puerto 80 sin forzar el uso de cifrado, dejando los datos vulnerables a ataques de interceptación.
[HIGH] Puerto 21 (FTP) ABIERTO: Protocolo de transferencia de archivos inseguro que expone nombres de usuario y contraseñas durante la transmisión.
[MEDIUM] Puerto 22 (SSH) ABIERTO: El servicio de administración remota está expuesto, lo cual es peligroso si no tiene políticas de bloqueo de IP o autenticación multifactor.
[MEDIUM] Puerto 8080 (HTTP-Alt) ABIERTO: Un puerto web alternativo está activo, lo que suele indicar la presencia de paneles de administración o servicios secundarios desprotegidos.
[LOW] Ausencia de robots.txt y sitemap.xml: No se encontraron archivos de guía para rastreadores, lo que indica una falta de configuración básica en el servidor web.