EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://intranet.pro-activa.es/es	Checks	9 pruebas
Dominio	intranet.pro-activa.es	Hallazgos	19 totales
Fecha	2 de septiembre de 2026 a las 13:32	Problemas	5 detectados

F

23/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha resultado en una puntuación crítica de 23/100, otorgando una calificación final de F. Se ejecutaron un total de 9 checks pasivos, de los cuales ninguno obtuvo un resultado satisfactorio, detectándose fallos graves en la infraestructura de cifrado y servicios expuestos. La ausencia de un certificado SSL válido y la apertura de puertos sensibles representan un riesgo inmediato para la integridad de los datos. En su estado actual, el sitio se clasifica como vulnerable y no apto para el manejo de información sensible o corporativa. Es imperativo realizar intervenciones técnicas urgentes para mitigar la superficie de ataque identificada.

Resumen de Riesgos

2	0	1	2	14
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	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 22 (SSH)...

SSL/TLS — 0/100

Estado: FALLO

Certificado SSL no valido

- CRITICO **Certificado valido**
  El certificado SSL NO es valido
- INFO **Dias hasta expiracion**
  64 dias restantes (expira: 2026-11-05T21:20:40.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-07T21:20:41.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://intranet.pro-activa.es/

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 — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 22 (SSH), 3306 (MySQL)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — Acceso remoto seguro
- INFO **Puerto 23 (Telnet)**
  Cerrado — 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
- 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] Certificado SSL no válido: La ausencia de un cifrado funcional permite ataques de interceptación de datos (Man-in-the-Middle) entre el usuario y el servidor.
[CRITICAL] Puerto 3306 (MySQL) abierto: El acceso directo a la base de datos desde internet facilita ataques de fuerza bruta y posible exfiltración de información confidencial.
[MEDIUM] Puerto 22 (SSH) abierto: La exposición del servicio de administración remota incrementa el riesgo de intentos de acceso no autorizado al sistema operativo.
[LOW] Ausencia de robots.txt y sitemap.xml: La falta de estos archivos impide una correcta gestión de la indexación y refleja una configuración web incompleta.
[ERROR] Fallo en verificación de cabeceras de seguridad: No se pudo confirmar la presencia de protecciones contra ataques de tipo XSS, Clickjacking o Inyección.
[ERROR] Fallo en configuración de cookies: No es posible garantizar que las sesiones de usuario estén protegidas con atributos de seguridad como Secure o HttpOnly.