EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://testfire.net	Checks	9 pruebas
Dominio	testfire.net	Hallazgos	19 totales
Fecha	27 de mayo de 2026 a las 02:57	Problemas	5 detectados

F

23/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio ha arrojado una puntuación crítica de 23/100, lo que corresponde a una nota de grado F. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales no se obtuvo ningún resultado satisfactorio, identificando 2 fallos críticos y 1 advertencia de seguridad. Los problemas principales radican en la invalidez del certificado SSL y la falta de redirección hacia conexiones seguras, sumado a la exposición de puertos no estándar. Debido a la ausencia de configuraciones de seguridad básicas y protecciones de cabecera, se concluye que el sitio es actualmente vulnerable. El estado de la plataforma representa un riesgo elevado para cualquier usuario que interactúe con ella.

Resumen de Riesgos

1	1	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	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 0/100

Estado: FALLO

Certificado SSL no valido

- CRITICO **Certificado valido**
  El certificado SSL NO es valido
- MEDIO **Dias hasta expiracion**
  26 dias restantes (expira: 2026-06-21T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-05-21T00:00:00.000Z
- 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 — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Certificado SSL inválido: El certificado de seguridad no es válido o ha expirado, lo que impide establecer una comunicación cifrada y confiable.
[HIGH] Ausencia de redirección HTTPS: El sitio permite conexiones a través de HTTP sin redirigir al protocolo seguro, exponiendo los datos a ataques de interceptación.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este puerto alternativo es peligrosa ya que suele utilizarse para servicios administrativos o proxies que carecen de las mismas protecciones que el puerto estándar.
[LOW] Fallo en robots.txt y sitemap.xml: No se pudo acceder a estos archivos, lo que indica una configuración deficiente del servidor y dificulta la auditoría de rutas indexadas.
[ERROR] Cabeceras de seguridad no verificadas: La plataforma no presenta configuraciones contra ataques de Cross-Site Scripting (XSS) o Clickjacking.
[ERROR] Seguridad de cookies no detectada: No se pudo confirmar el uso de etiquetas de seguridad en cookies, lo que podría facilitar el robo de sesiones.