EscanearVulnerabilidades

Informe de Seguridad Web

URL	http://demo.testfire.net/	Checks	9 pruebas
Dominio	demo.testfire.net	Hallazgos	43 totales
Fecha	10 de julio de 2026 a las 17:24	Problemas	16 detectados

F

36/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio demo.testfire.net ha arrojado una puntuación de 36/100, lo que resulta en una calificación de insuficiencia total con una nota F. Durante el proceso se ejecutaron 9 checks pasivos, identificando 4 fallos críticos, 2 advertencias y solo 2 validaciones correctas. La ausencia de un cifrado SSL válido y la carencia absoluta de cabeceras de seguridad modernas exponen al sitio y a sus usuarios a riesgos graves de interceptación y robo de datos. Debido a estas deficiencias estructurales en la configuración del servidor, el sitio se concluye como altamente vulnerable y no apto para el manejo de información sensible.

Resumen de Riesgos

1	7	5	3	27
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	33	FALLO	JSESSIONID: falta Secure; JSESSIONID: falta Same...
Contenido Mixto	50	AVISO	El sitio no usa HTTPS, no aplica chequeo de cont...
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
- ALTO **Dias hasta expiracion**
  -19 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

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache-Coyote/1.1 — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

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

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 33/100

Estado: FALLO

JSESSIONID: falta Secure; JSESSIONID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: JSESSIONID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript

- ALTO **Cookie: JSESSIONID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: JSESSIONID — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 50/100

Estado: AVISO

El sitio no usa HTTPS, no aplica chequeo de contenido mixto

- ALTO **Protocolo**
  El sitio no usa HTTPS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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 no válido: El certificado SSL ha expirado hace 19 días, lo que impide establecer conexiones cifradas confiables y genera alertas de seguridad en los navegadores.
[HIGH] Ausencia de redirección HTTPS: El sitio permite conexiones a través de HTTP sin redirigir al protocolo seguro, facilitando ataques de hombre en el medio (MitM).
[HIGH] Falta de Content-Security-Policy (CSP): El sitio carece de una política de seguridad de contenido, lo que lo hace vulnerable a ataques de inyección como Cross-Site Scripting (XSS).
[HIGH] Falta de X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea embebido en frames de dominios externos, facilitando ataques de clickjacking.

[HIGH] Falta de Strict-Transport-Security (HSTS): No se fuerza el uso de HTTPS, permitiendo que las comunicaciones puedan ser degradadas a protocolos no cifrados.
[HIGH] Cookie de sesión insegura (JSESSIONID): La cookie carece del flag Secure, lo que significa que el identificador de sesión puede ser transmitido a través de conexiones HTTP no cifradas.
[MEDIUM] Vulnerabilidad a CSRF en Cookies: La cookie JSESSIONID no implementa el atributo SameSite, permitiendo que un atacante realice peticiones no autorizadas en nombre del usuario.
[MEDIUM] Falta de X-Content-Type-Options: El servidor no previene el MIME-type sniffing, lo que podría permitir al navegador interpretar archivos de forma maliciosa.
[MEDIUM] Falta de Referrer-Policy: No existe control sobre la información de referencia que se envía al navegar hacia otros sitios, comprometiendo la privacidad de los usuarios.
[MEDIUM] Puerto 8080 expuesto: Se detectó el puerto 8080 abierto, el cual suele ser utilizado para servicios de administración o proxies que aumentan la superficie de ataque.
[LOW] Cabecera Server expuesta: Se revela el uso de Apache-Coyote/1.1, información técnica que ayuda a potenciales atacantes a buscar exploits específicos para esa tecnología.
[LOW] Ausencia de archivos de rastreo: No se encontraron los archivos robots.txt ni sitemap.xml, lo que indica una falta de configuración básica en la gestión de contenidos y visibilidad del sitio.