EscanearVulnerabilidades

Informe de Seguridad Web

URL	http://silfius.ddns.net	Checks	9 pruebas
Dominio	silfius.ddns.net	Hallazgos	13 totales
Fecha	29 de junio de 2026 a las 09:49	Problemas	1 detectados

B

75/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre silfius.ddns.net arroja una puntuación de 75/100, lo que corresponde a una nota de B. Se ejecutaron 9 checks pasivos, de los cuales 1 resultó correcto y 1 generó una advertencia de riesgo. La evaluación se vio limitada por múltiples tiempos de espera agotados que impidieron la verificación de parámetros críticos como las cabeceras y las cookies. Concluimos que el sitio es vulnerable debido a la ausencia de cifrado en las comunicaciones. Este estado representa un riesgo para la integridad de cualquier dato que se intercambie con el servidor.

Resumen de Riesgos

0	1	0	0	12
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

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	50	AVISO	El sitio no usa HTTPS, no aplica chequeo de cont...
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

Contenido Mixto — 50/100

Estado: AVISO

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

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

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

[ALTA] Protocolo: El sitio no utiliza HTTPS, lo que significa que la información viaja en texto plano y puede ser interceptada por terceros.
[MEDIA] Contenido Mixto: Al no disponer de una conexión segura, no es posible aplicar políticas de contenido mixto, dejando la sesión sin garantías de autenticidad.
[BAJA] Fallos de Verificación: Se detectaron errores de tiempo de espera (timeout) al intentar analizar cabeceras de seguridad y versiones de software, lo que sugiere una configuración de red inestable o restrictiva.