EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://tecnetsv.com/	Checks	9 pruebas
Dominio	tecnetsv.com	Hallazgos	42 totales
Fecha	12 de mayo de 2026 a las 22:37	Problemas	11 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio tecnetsv.com ha resultado en una puntuación de 73/100, lo que otorga una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo 5 resultados satisfactorios, 2 advertencias y 2 fallos en áreas críticas de configuración. Aunque la capa de cifrado inicial es sólida, la exposición de servicios de infraestructura y la carencia de políticas de seguridad en el servidor representan un riesgo latente. Por lo tanto, el sitio se clasifica actualmente como vulnerable debido a la visibilidad pública de puertos sensibles y la falta de cabeceras de protección.

Resumen de Riesgos

1	4	3	3	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 36 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 36 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  36 dias restantes (expira: 2026-06-18T08:46:29.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-20T08:46:30.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: LiteSpeed — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://tecnetsv.com/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

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 — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por 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

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- 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] Puerto 3306 (MySQL): El servicio de base de datos está abierto al exterior, permitiendo intentos de conexión remota y ataques de fuerza bruta contra los datos.
[HIGH] Puerto 21 (FTP): El puerto de transferencia de archivos está activo y accesible, lo que facilita la interceptación de credenciales y archivos al no utilizar cifrado por defecto.
[HIGH] Strict-Transport-Security (HSTS): Falta la configuración de HSTS, lo que impide que el sitio obligue a los navegadores a usar siempre conexiones seguras.
[HIGH] X-Frame-Options: La ausencia de esta cabecera hace que el sitio sea susceptible a ataques de Clickjacking, permitiendo que terceros lo carguen dentro de marcos maliciosos.
[MEDIUM] X-Content-Type-Options: No se ha implementado la directiva para evitar que el navegador realice sniffing de tipos MIME, lo que podría derivar en la ejecución de scripts maliciosos.

[MEDIUM] Referrer-Policy: La falta de esta política de seguridad impide controlar qué información de navegación se comparte con otros dominios.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a funciones del navegador como la ubicación o periféricos, aumentando la superficie de ataque.
[LOW] Server header expuesto: El servidor responde con la firma LiteSpeed, revelando la tecnología subyacente y facilitando la búsqueda de vulnerabilidades específicas para esa versión.
[LOW] robots.txt y sitemap.xml: La falta de estos archivos genera errores 404 y dificulta el control sobre el rastreo de los motores de búsqueda.