EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.tecno12-18.com/lm/index.asp	Checks	9 pruebas
Dominio	www.tecno12-18.com	Hallazgos	49 totales
Fecha	7 de mayo de 2026 a las 18:39	Problemas	17 detectados

C

63/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 63/100, lo que equivale a una nota de C. El análisis se basó exclusivamente en 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 3 generaron advertencias y 2 fueron calificados como fallos críticos. Aunque el cifrado de transporte es correcto, la ausencia total de cabeceras de seguridad y la exposición de servicios obsoletos elevan el riesgo operativo. Debido a las deficiencias en la protección de cookies y la apertura de puertos inseguros, se concluye que el sitio es vulnerable a ataques de interceptación y secuestro de sesiones. Es imperativo aplicar medidas correctivas para alcanzar un nivel de protección adecuado.

Resumen de Riesgos

0	6	10	1	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 153 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
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	33	FALLO	ASPSESSIONIDCGRDARTA: falta HttpOnly; ASPSESSION...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 153 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  153 dias restantes (expira: 2026-10-07T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-23T00:00:00.000Z
- 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: Microsoft-IIS/10.0 — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://www.tecno12-18.com/index.asp
- 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

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente

- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 33/100

Estado: FALLO

ASPSESSIONIDCGRDARTA: falta HttpOnly; ASPSESSIONIDCGRDARTA: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: ASPSESSIONIDCGRDARTA — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: ASPSESSIONIDCGRDARTA — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: ASPSESSIONIDCGRDARTA — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (100 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 4 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- 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
- 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

[HIGH] Falta de Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking, permitiendo que atacantes carguen la web en marcos externos para engañar al usuario.
[HIGH] Falta de Strict-Transport-Security: No se fuerza el uso de HTTPS en el navegador, lo que facilita ataques de degradación de conexión.
[HIGH] Cookie de sesión insegura (HttpOnly): La cookie ASPSESSIONIDCGRDARTA carece del atributo HttpOnly, permitiendo que sea robada mediante scripts maliciosos.
[HIGH] Puerto 21 (FTP) abierto: Este servicio transfiere datos y credenciales en texto plano, siendo altamente vulnerable a interceptaciones.
[MEDIUM] Falta de X-Content-Type-Options: El sitio no previene el sniffing de tipos MIME, lo que podría llevar a la ejecución de archivos con contenido inesperado.
[MEDIUM] Falta de Referrer-Policy: No se controla la información de procedencia enviada a sitios externos, pudiendo filtrar rutas privadas.
[MEDIUM] Falta de Permissions-Policy: El navegador no tiene restricciones para acceder a APIs sensibles como la cámara o el micrófono.
[MEDIUM] Cookie de sesión insegura (SameSite): La falta de este atributo hace que el sitio sea susceptible a ataques de falsificación de solicitudes entre sitios (CSRF).
[MEDIUM] Archivos y rutas informativas expuestas: La presencia de archivos como /readme.html y paneles de acceso como /administrator/ facilita el reconocimiento para atacantes.
[MEDIUM] Configuración restrictiva en robots.txt: Se bloquea el rastreo completo del sitio, lo cual es una práctica inusual que no sustituye la seguridad real.
[LOW] Cabecera Server expuesta: Se revela el uso de Microsoft-IIS/10.0, proporcionando información técnica valiosa para explotar vulnerabilidades específicas del software.