EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.t-mobile.com/	Checks	9 pruebas
Dominio	www.t-mobile.com	Hallazgos	49 totales
Fecha	18 de septiembre de 2026 a las 13:40	Problemas	9 detectados

C

66/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al dominio ha resultado en una puntuación de 66/100, lo que otorga una calificación de grado C. Durante la evaluación se ejecutaron un total de 9 controles pasivos, obteniendo 6 resultados satisfactorios, 1 advertencia y 2 fallos críticos en la configuración del servidor. El sitio web presenta deficiencias notables en la implementación de cabeceras de seguridad y en la gestión de redirecciones de tráfico cifrado. Debido a estos hallazgos, el sitio se considera vulnerable a ataques de interceptación y manipulación de datos, requiriendo intervención técnica inmediata.

Resumen de Riesgos

0	4	4	1	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 152 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a 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	67	AVISO	akacd_www_t_mobile_com_phased_release_non_shared...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 152 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  152 dias restantes (expira: 2027-02-17T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-03T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido

- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000 ; includeSubDomains ; preload
- 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: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 403 — No redirige a HTTPS
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000 ; includeSubDomains ; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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 — 67/100

Estado: AVISO

akacd_www_t_mobile_com_phased_release_non_shared: falta HttpOnly

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: akacd_www_t_mobile_com_phased_release_non_shared — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: akacd_www_t_mobile_com_phased_release_non_shared — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: akacd_www_t_mobile_com_phased_release_non_shared — SameSite**
  SameSite=none

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (3392 bytes)
- INFO **Reglas robots.txt**
  53 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.t-mobile.com/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[ALTA] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking donde un atacante puede cargar la web en un marco invisible.
[ALTA] Redirección HTTPS: El servidor no redirige automáticamente el tráfico HTTP a HTTPS, devolviendo un error 403 y exponiendo a los usuarios a conexiones no seguras.
[ALTA] Cookie vulnerable: La cookie akacd_www_t_mobile_com_phased_release_non_shared carece del atributo HttpOnly, permitiendo su robo mediante scripts de terceros.
[MEDIA] X-Content-Type-Options: La falta de esta directiva permite al navegador realizar MIME-sniffing, lo que podría derivar en la ejecución de archivos con contenido malicioso.
[MEDIA] Referrer-Policy: No existe control sobre la información de procedencia enviada a otros dominios, lo que podría filtrar datos de navegación sensibles.
[MEDIA] Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como la cámara o el micrófono, aumentando la superficie de ataque en el cliente.
[MEDIA] Divulgación de rutas en robots.txt: Se expone la ruta admin dentro del archivo de configuración para buscadores, facilitando la identificación de áreas restringidas.
[BAJA] Bloqueo total en robots.txt: El archivo impide el indexado completo del sitio mediante la instrucción Disallow, lo que podría ser una configuración errónea o restrictiva.