EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://account.t-mobile.com/signin/v2/?client_id=SMG_PROD&response_type=code&prompt=...	Checks	8 pruebas
Dominio	account.t-mobile.com	Hallazgos	42 totales
Fecha	12 de septiembre de 2026 a las 15:51	Problemas	8 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el sitio web arroja una puntuación de 65/100, lo que corresponde a una calificación de grado C. Durante la evaluación, se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 presentaron fallos críticos que comprometen la integridad de la plataforma. Se han detectado debilidades importantes en la configuración de cabeceras de seguridad y en la gestión de protocolos de conexión cifrada. Debido a la ausencia de mecanismos de protección contra ataques de inyección y suplantación, el sitio se considera vulnerable en su estado actual. Se requiere una intervención inmediata para elevar los estándares de protección a un nivel aceptable.

Resumen de Riesgos

0	3	4	1	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 49 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	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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 49 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  49 dias restantes (expira: 2026-10-31T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-16T00:00:00.000Z
- 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
- 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
- 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)
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- 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 **sitemap.xml**
  No encontrado (HTTP 403)
- 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

[HIGH] Content-Security-Policy: Falta — Su ausencia permite la ejecución de scripts maliciosos, ataques de Cross-Site Scripting (XSS) e inyección de contenido.
[HIGH] X-Frame-Options: Falta — El sitio es vulnerable a ataques de clickjacking, permitiendo que atacantes carguen la página en marcos invisibles para engañar al usuario.
[HIGH] HTTP a HTTPS redireccion: FAIL — El servidor no redirige automáticamente el tráfico inseguro al protocolo cifrado, respondiendo con un error 403 en su lugar.
[MEDIUM] X-Content-Type-Options: Falta — No se previene el MIME-type sniffing, lo que podría permitir al navegador interpretar archivos de forma incorrecta y ejecutar código malicioso.
[MEDIUM] Referrer-Policy: Falta — No se controla la información de procedencia enviada en las peticiones, lo que puede exponer URLs internas sensibles.
[MEDIUM] Permissions-Policy: Falta — El sitio no restringe el acceso de las APIs del navegador a componentes de hardware como la cámara o el micrófono.
[MEDIUM] Archivo /README.txt: Accesible — La exposición de este archivo puede revelar detalles técnicos sobre el entorno y la estructura interna del servidor.

[LOW] sitemap.xml y robots.txt: No encontrados — La falta de estos archivos dificulta la auditoría de rutas permitidas y la indexación controlada por parte de buscadores.