EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://es.account.t-mobile.com/signin/v2/?redirect_uri=https:%2F%2Fes.account.t-mobile.com%2Fsignin&scope=TMO_ID_profile%2520associated_lines%2520ban_roles%2520billing_information%2520associated_billing_accounts%2520extended_lines%2520token%2520openid%2520vault%2520role%2520consent&client_id=MYTMO&access_type=ONLINE&response_type=code&approval_prompt=auto&prompt=select_account&state=eyJpbnRlbnQiOiJMb2dpbiIsImJvb2ttYXJrVXJsIjoiaHR0cHM6Ly9lcy50LW1vYmlsZS5jb20vYWNjb3VudC9kYXNoYm9hcmQifQ	Crawl	9 páginas
Dominio	es.account.t-mobile.com	Hallazgos	42 totales
Fecha	12 de septiembre de 2026 a las 21:08	Problemas	8 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar la auditoría técnica, el sitio web presenta una puntuación de 65/100, lo que equivale a una nota de C. Se ejecutaron un total de 9 controles pasivos, de los cuales 6 resultaron satisfactorios, mientras que 3 presentaron fallos críticos en su configuración. El análisis revela carencias importantes en la implementación de cabeceras de seguridad y fallos en la redirección obligatoria hacia protocolos cifrados. Por lo tanto, se concluye que el sitio es vulnerable ante ataques de inyección y suplantación de identidad.

Resumen de Riesgos

0	3	4	1	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 139 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 139 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  139 dias restantes (expira: 2027-01-29T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-30T00:00:00.000Z
- 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=15768000 ; 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=15768000 ; preload
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=15768000 (183 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: Esta cabecera no está configurada, facilitando la ejecución de ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: La ausencia de este control permite que el sitio sea embebido en marcos externos, aumentando el riesgo de ataques de clickjacking.
[HIGH] Redirección HTTP a HTTPS: El servidor no redirige automáticamente las peticiones inseguras a una conexión cifrada, respondiendo con un error 403.
[MEDIUM] X-Content-Type-Options: Al faltar esta cabecera, el navegador podría realizar sniffing de tipos MIME, permitiendo la ejecución involuntaria de scripts ocultos.
[MEDIUM] Referrer-Policy: No se define una política para el envío de información de referencia, lo que podría exponer rutas internas a terceros.
[MEDIUM] Permissions-Policy: La falta de restricción en las APIs del navegador permite que el sitio acceda potencialmente a funciones de hardware sin un control estricto.
[MEDIUM] Archivo /README.txt: Se detectó un archivo técnico accesible públicamente que podría revelar información sensible sobre el desarrollo o estructura del portal.

[LOW] sitemap.xml: El archivo no fue localizado en la ruta esperada, impidiendo una correcta validación de la estructura pública del sitio.