EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://smgui.t-mobile.com/smg-ui/login?code=M.C504_BAY.2.U.MsaArtifacts.Dj ... czqWevam3Nl8bu3OtspRr2kX80tVWGZJG0FVI1Qo%24&state=b76de5-h85-e1d-0b-b02ba3a8	Checks	9 pruebas
Dominio	smgui.t-mobile.com	Hallazgos	47 totales
Fecha	12 de septiembre de 2026 a las 16:31	Problemas	12 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web ha dado como resultado una puntuación exacta de 73/100, lo que otorga una calificación de nota C. Durante la auditoría, se ejecutaron 9 checks pasivos, obteniendo 6 resultados satisfactorios, 0 advertencias y 3 fallos críticos en configuraciones de red y aplicación. Aunque el cifrado de datos es sólido, la ausencia de cabeceras de seguridad fundamentales y la configuración incompleta de cookies exponen a los usuarios a riesgos interceptables. Por lo tanto, el sitio se considera actualmente vulnerable ante ataques de inyección y suplantación de identidad. Es imperativo aplicar las correcciones técnicas detalladas para mejorar la postura de seguridad global.

Resumen de Riesgos

0	3	9	0	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 41 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	ak_bmsc: falta Secure; ak_bmsc: falta SameSite
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 41 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  41 dias restantes (expira: 2026-10-23T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-08T00:00:00.000Z
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://smgui.t-mobile.com/
- 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 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

ak_bmsc: falta Secure; ak_bmsc: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: ak_bmsc — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: ak_bmsc — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: ak_bmsc — 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 — 20/100

Estado: FALLO

Faltan robots.txt y 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

[HIGH] Content-Security-Policy: Falta esta cabecera, la cual es vital para prevenir ataques de Cross-Site Scripting (XSS) e inyecciones de contenido malicioso.
[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea cargado en marcos externos, facilitando ataques de clickjacking.
[HIGH] Cookie ak_bmsc (Secure): La cookie carece del flag Secure, lo que significa que puede ser transmitida a través de conexiones HTTP no cifradas.
[MEDIUM] X-Content-Type-Options: Falta la configuración para evitar que el navegador realice MIME-type sniffing, lo que podría llevar a la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No existe una política definida para controlar cuánta información de referencia se envía a otros sitios web.
[MEDIUM] Permissions-Policy: No se han restringido las APIs del navegador, permitiendo potencialmente el acceso no autorizado a hardware como cámara o micrófono.
[MEDIUM] Cookie ak_bmsc (SameSite): La falta del atributo SameSite hace que la sesión sea vulnerable a ataques de Cross-Site Request Forgery (CSRF).
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y puede revelar información técnica sensible sobre la infraestructura del sitio.
[MEDIUM] Archivo /README.txt: Documento técnico expuesto que facilita a un atacante potencial la identificación de versiones de software.
[MEDIUM] Ruta /wp-login.php: Se detectó un panel de inicio de sesión accesible, lo que aumenta la superficie de ataque para intentos de fuerza bruta.
[MEDIUM] Ruta /administrator/: Panel administrativo expuesto que representa un riesgo de acceso no autorizado si no está debidamente protegido.
[MEDIUM] Ruta /user/login: Punto de entrada de usuarios visible públicamente que requiere medidas de seguridad adicionales.
[LOW] Robots.txt y Sitemap: La ausencia de estos archivos dificulta la auditoría de rutas permitidas y afecta la visibilidad controlada del sitio.