EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://helm.tekmob.com/pim/attmyaccount	Checks	9 pruebas
Dominio	helm.tekmob.com	Hallazgos	49 totales
Fecha	28 de abril de 2026 a las 19:03	Problemas	16 detectados

D

52/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha resultado en una puntuación de 52/100, lo que otorga una calificación de grado D. Durante el análisis se ejecutaron 9 checks pasivos, obteniendo 4 resultados satisfactorios, 2 advertencias y 3 fallos críticos en la configuración. Aunque el cifrado de transporte cuenta con un certificado válido, existen deficiencias graves en la protección de las sesiones de usuario y en la implementación de políticas de seguridad en el navegador. Debido a la ausencia de mecanismos básicos de defensa y la exposición de información del servidor, se concluye que el sitio es actualmente vulnerable ante ataques de interceptación y manipulación de datos.

Resumen de Riesgos

0	6	7	3	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 298 dias
Cabeceras de Seguridad	15	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	0	FALLO	JSESSIONID: falta HttpOnly; JSESSIONID: falta Se...
Contenido Mixto	60	AVISO	3 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 298 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  298 dias restantes (expira: 2027-02-20T11:38:52.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-16T15:05:01.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: Apache-Coyote/1.1 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1 — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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
- INFO **Tecnologias detectadas**
  Servlet 2.5; JBoss-5.0/JBossWeb-2.1

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 — 0/100

Estado: FALLO

JSESSIONID: falta HttpOnly; JSESSIONID: falta Secure; JSESSIONID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: JSESSIONID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: JSESSIONID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: JSESSIONID — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

3 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://helm.tekmob.com/pimmexm3p/m6298574_b122.png
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.timwe.com/sites/timwe.com/themes/timwe/favicon.ic...
- MEDIO **Recurso HTTP (form action)**
  http://helm.tekmob.com/pim/attmyaccount

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (45 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- BAJO **sitemap.xml**
  Error al acceder

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] Falta de redirección HTTP a HTTPS: El sitio permite conexiones no cifradas, lo que expone los datos de los usuarios a ataques de intermediario (MitM).
[HIGH] Ausencia de Strict-Transport-Security (HSTS): No se instruye al navegador para que utilice exclusivamente conexiones seguras, permitiendo degradaciones de protocolo.
[HIGH] Cookies de sesión inseguras (JSESSIONID): La cookie carece de los flags HttpOnly y Secure, permitiendo su robo mediante scripts maliciosos o conexiones no cifradas.
[HIGH] Falta de Content-Security-Policy (CSP): El sitio no tiene protección contra ataques de Cross-Site Scripting (XSS) e inyección de contenido.
[MEDIUM] Cookie sin atributo SameSite: La falta de este flag en JSESSIONID hace que el sitio sea vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido mixto (Mixed Content): Se detectaron 3 recursos, incluyendo imágenes y formularios, que se cargan vía HTTP dentro de la página HTTPS, comprometiendo la integridad.
[MEDIUM] Falta de X-Content-Type-Options: El sitio es vulnerable al sniffing de tipos MIME, lo que podría permitir la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Ausencia de Referrer-Policy y Permissions-Policy: No existe control sobre la información de navegación compartida ni sobre el acceso a APIs sensibles del dispositivo.
[LOW] Exposición de cabeceras de servidor: Las cabeceras Server y X-Powered-By revelan el uso de Apache-Coyote/1.1 y JBoss-5.0, facilitando la búsqueda de exploits específicos.
[LOW] Falta de Sitemap: La ausencia del archivo sitemap.xml dificulta la auditoría completa de la estructura del sitio y su correcta indexación.