EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.tecsiscom.com/tienda/	Checks	9 pruebas
Dominio	www.tecsiscom.com	Hallazgos	51 totales
Fecha	26 de septiembre de 2026 a las 20:54	Problemas	16 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha arrojado una puntuación de 65/100, obteniendo una calificación de grado C. Se realizaron 9 checks pasivos de los cuales 4 resultaron exitosos, 2 presentaron advertencias y 3 fallaron en criterios de seguridad críticos. Aunque el cifrado de transporte es correcto, se detectaron fallos importantes en la configuración de cabeceras y exposición de puertos. En su estado actual, el sitio se considera vulnerable debido a la posibilidad de ataques de interceptación de datos y ataques dirigidos al cliente.

Resumen de Riesgos

0	3	9	4	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 77 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	CMS detectado: PrestaShop
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	67	AVISO	PrestaShop-80bed873bef4c8487ed55c4f9d81457b: fal...
Contenido Mixto	20	FALLO	8 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 77 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  77 dias restantes (expira: 2026-12-13T00:46:05.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-14T00:46:06.000Z
- 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

- BAJO **Server header expuesto**
  Server: nginx — Revela tecnologia del servidor

- 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;
- 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://www.tecsiscom.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000;
- BAJO **HSTS includeSubDomains**
  HSTS no 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

CMS detectado: PrestaShop

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: PrestaShop

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

PrestaShop-80bed873bef4c8487ed55c4f9d81457b: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: PrestaShop-80bed873bef4c8487ed55c4f9d81457b — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: PrestaShop-80bed873bef4c8487ed55c4f9d81457b — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: PrestaShop-80bed873bef4c8487ed55c4f9d81457b — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 20/100

Estado: FALLO

8 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.tecsiscom.com/tienda
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.tecsiscom.com/tienda/index.php?id_product=610&amp...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.tecsiscom.com/tienda/index.php?id_product=478&amp...
- MEDIO **href (link/stylesheet)**
  ...y 5 mas del mismo tipo

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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 no autorizados y ataques de inyección de contenido XSS.
[ALTA] X-Frame-Options: Al no estar implementada, el sitio es susceptible a ataques de clickjacking donde un atacante puede camuflar la interfaz.
[ALTA] Puerto 21 (FTP): Este puerto está abierto y permite la transferencia de archivos de forma no cifrada, exponiendo credenciales en la red.
[MEDIA] Contenido Mixto: Se detectaron 8 recursos cargados mediante HTTP en una página HTTPS, lo que debilita la integridad de la conexión cifrada.
[MEDIA] Cookie SameSite: La cookie de PrestaShop carece del atributo SameSite, lo que facilita ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIA] X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido, facilitando ataques de sniffing.
[MEDIA] Referrer-Policy: No existe control sobre la información de referencia enviada a terceros, lo que podría filtrar URLs privadas.
[MEDIA] Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono.
[MEDIA] Puerto 22 (SSH): El servicio de acceso remoto está expuesto públicamente, aumentando el riesgo de ataques de fuerza bruta.
[BAJA] Server header expuesto: El servidor revela el uso de nginx, proporcionando información útil a posibles atacantes para buscar vulnerabilidades específicas.
[BAJA] Meta generator: El código fuente expone que el sitio utiliza PrestaShop, lo que ayuda a perfilar el sistema.
[BAJA] Robots.txt y Sitemap: La ausencia de estos archivos dificulta la auditoría de rutas y la correcta indexación de seguridad.