

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://temu.com
Dominio temu.com
Fecha 2 de junio de 2026 a las 18:41

Checks 9 pruebas
Hallazgos 45 totales
Problemas 8 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del dominio temu.com ha arrojado una puntuación de 80/100, lo que corresponde a una nota B. Se realizaron 9 checks pasivos, resultando en 7 verificaciones exitosas y 2 fallos críticos relacionados con la configuración de seguridad del servidor y archivos de indexación. Aunque el sitio demuestra una base sólida en cuanto a cifrado de datos y redirecciones seguras, presenta carencias importantes en la implementación de cabeceras de defensa del navegador. En conclusión, el sitio se considera seguro en su infraestructura básica, pero vulnerable ante ataques específicos de inyección de código y clickjacking.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 73 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	100	OK	1 cookies, todas con flags correctos
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 73 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
73 dias restantes (expira: 2026-08-14T08:24:19.000Z)
- INFO **Fecha de emision**
Emitido desde: 2025-07-13T21:18:28.000Z
- 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: cloudflare — 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://temu.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

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
- **INFO** **Version CMS**
No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
1 cookie(s) encontrada(s)
- INFO **Cookie: __cf_bm — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __cf_bm — SameSite**
SameSite=none

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: La ausencia de esta cabecera impide mitigar ataques de Cross-Site Scripting (XSS) y otros ataques de inyección de contenido malicioso.

[HIGH] X-Frame-Options: Esta cabecera no está configurada, lo que deja al sitio expuesto a ataques de clickjacking mediante el uso de marcos o iframes.

[MEDIUM] X-Content-Type-Options: La falta de esta política permite el MIME-type sniffing, pudiendo engañar al navegador para que ejecute scripts maliciosos.

[MEDIUM] Referrer-Policy: No existe control sobre la información de procedencia enviada en las peticiones salientes, lo que compromete la privacidad de la navegación.

[MEDIUM] Permissions-Policy: Al no estar definida, no se restringe el acceso a APIs sensibles del dispositivo del usuario como cámara, micrófono o geolocalización.

[MEDIUM] Exposición de archivos /readme.html y /README.txt: Estos archivos son accesibles públicamente y pueden revelar información técnica sobre el entorno o la plataforma.

[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, lo que proporciona información sobre la infraestructura de red a posibles atacantes.

[LOW] Ausencia de robots.txt y sitemap.xml: El sitio carece de estos archivos, lo que dificulta la indexación controlada y el análisis estructurado de la web.