EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://tienda.cumminsperu.pe/	Checks	9 pruebas
Dominio	tienda.cumminsperu.pe	Hallazgos	53 totales
Fecha	31 de marzo de 2026 a las 22:03	Problemas	11 detectados

C

74/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación técnica de 74/100, lo que equivale a una nota de C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron exitosos, 3 generaron advertencias y 1 fue identificado como fallo crítico. Los principales problemas detectados se centran en la ausencia de cabeceras de seguridad y una configuración deficiente en el manejo de cookies. Aunque el cifrado de datos es robusto, la falta de políticas de protección contra ataques de inyección y suplantación permite concluir que el sitio es vulnerable a ataques dirigidos.

Resumen de Riesgos

0	4	5	2	42
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 82 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 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	50	AVISO	frontend_lang: falta HttpOnly; frontend_lang: fa...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 82 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  82 dias restantes (expira: 2026-06-22T04:36:57.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-24T04:36:58.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Odoo.sh — 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; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff, nosniff
- 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://tienda.cumminsperu.pe/
- 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
- BAJO **Meta generator**
  Expone: Odoo
- INFO **Tecnologias detectadas**
  Next.js

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 — 50/100

Estado: AVISO

frontend_lang: falta HttpOnly; frontend_lang: falta Secure; frontend_lang: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: frontend_lang — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: frontend_lang — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: frontend_lang — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: session_id — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: session_id — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: session_id — SameSite**
  SameSite=lax

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://tienda.contacto@cumminsperu.pe

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (116 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://tienda.cumminsperu.pe/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — 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

[HIGH] Falta de Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] Falta de X-Frame-Options: El sitio es susceptible a ataques de clickjacking, permitiendo que un atacante cargue la web en marcos invisibles para engañar al usuario.
[HIGH] Cookie frontend_lang sin flag HttpOnly: Esta omisión permite que scripts maliciosos accedan a la cookie a través del navegador, aumentando el riesgo de robo de sesión.
[HIGH] Cookie frontend_lang sin flag Secure: Al no tener este flag, la cookie podría transmitirse a través de conexiones no cifradas, exponiendo datos sensibles.
[MEDIUM] Falta de Referrer-Policy: No se controla la información de procedencia enviada a terceros, lo que puede filtrar URLs privadas o datos de navegación.
[MEDIUM] Falta de Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Cookie frontend_lang sin flag SameSite: Esta configuración hace que el sitio sea vulnerable a ataques de falsificación de solicitud en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto detectado: Se identificó un recurso cargando mediante HTTP (tienda.contacto@cumminsperu.pe), lo que compromete la integridad de la conexión segura.
[MEDIUM] Puerto 22 (SSH) abierto: La exposición de este puerto de administración remota incrementa la superficie de ataque para intentos de acceso por fuerza bruta.
[LOW] Cabecera de servidor expuesta (Odoo.sh): Revela la tecnología específica utilizada, facilitando a un atacante la búsqueda de vulnerabilidades conocidas para esa plataforma.
[LOW] Etiqueta Meta Generator expuesta: El código fuente confirma el uso de Odoo, proporcionando información valiosa para la fase de reconocimiento de un ciberdelincuente.