EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://orderatphone.com	Checks	9 pruebas
Dominio	orderatphone.com	Hallazgos	51 totales
Fecha	22 de junio de 2026 a las 13:09	Problemas	8 detectados

B

79/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio orderatphone.com arroja una puntuación de 79/100, lo que equivale a una calificación de nota B. Se ejecutaron 9 checks pasivos que resultaron en 5 verificaciones correctas, 3 advertencias por configuraciones mejorables y 1 fallo crítico en la implementación de cabeceras de seguridad. La plataforma demuestra una gestión sólida del cifrado de datos y el protocolo HTTPS, aunque presenta deficiencias en la protección contra ataques de inyección y exposición de puertos administrativos. Con base en estos resultados, se concluye que el sitio es funcionalmente seguro en el transporte de información, pero vulnerable a ataques dirigidos al cliente y a la sesión del usuario.

Resumen de Riesgos

0	2	4	2	43
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 51 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	83	AVISO	XSRF-TOKEN: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 51 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  51 dias restantes (expira: 2026-08-12T13:04:33.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-14T13:04:34.000Z
- 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-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
- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=315360000; 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://orderatphone.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=315360000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=315360000 (3650 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

- 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 — 83/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: OAP_AUX_TOKEN — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: OAP_AUX_TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: OAP_AUX_TOKEN — SameSite**
  SameSite=lax

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (24 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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] Content-Security-Policy: La ausencia de esta cabecera impide prevenir ataques de Cross-Site Scripting (XSS) e inyecciones de código malicioso en el navegador del usuario.
[HIGH] Cookie XSRF-TOKEN: El token de seguridad carece del atributo HttpOnly, lo que permite que sea accesible mediante scripts y facilita el robo de la sesión.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador podría interpretar archivos de forma incorrecta, permitiendo ataques de tipo MIME-sniffing.
[MEDIUM] Referrer-Policy: La falta de esta política puede causar la filtración involuntaria de información de navegación hacia sitios de terceros.
[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de APIs del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Puerto 22 (SSH) abierto: La exposición externa de este puerto de administración remota aumenta el riesgo de intentos de acceso no autorizado mediante fuerza bruta.
[LOW] Server header expuesto: El servidor responde revelando explícitamente que utiliza nginx, facilitando la búsqueda de exploits específicos para esa tecnología.
[LOW] sitemap.xml ausente: El archivo de mapa del sitio no fue encontrado, lo que afecta la organización de los recursos indexables del servidor.