EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.es.ebay.com/	Checks	9 pruebas
Dominio	www.es.ebay.com	Hallazgos	79 totales
Fecha	5 de junio de 2026 a las 13:35	Problemas	32 detectados

C

66/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web ha resultado en una puntuación de 66/100, lo que otorga una nota de calificación C. El análisis se basó en 9 checks pasivos de los cuales 5 fueron satisfactorios, 1 presentó advertencias y 3 fallaron en aspectos críticos de configuración. A pesar de contar con un cifrado SSL robusto, se han detectado debilidades importantes en la gestión de cookies y en la ausencia de cabeceras de seguridad preventivas. Se concluye que el sitio es actualmente vulnerable debido a fallos en la redirección de tráfico y a la exposición de vectores de ataque por configuración insuficiente. El nivel de riesgo identificado requiere medidas correctivas para elevar los estándares de protección del dominio.

Resumen de Riesgos

0	16	15	1	47
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 139 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 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	27	FALLO	nonsession: falta SameSite; s: falta SameSite; d...
Contenido Mixto	100	OK	No se detecto contenido mixto
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 139 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  139 dias restantes (expira: 2026-10-22T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-07T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: ebay-proxy-server — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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 301 — No redirige a HTTPS
- 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
- INFO **Tecnologias detectadas**
  Next.js, Astro

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 — 27/100

Estado: FALLO

nonsession: falta SameSite; s: falta SameSite; ds2: falta HttpOnly; ebay: falta HttpOnly; ebay: falta SameSite; __deba: falta SameSite; __uzma: falta HttpOnly; __uzma: falta Secure; __uzma: falta SameSite; __uzmb: falta HttpOnly; __uzmb: falta Secure; __uzmb: falta SameSite; __uzmc: falta HttpOnly; __uzmc: falta Secure; __uzmc: falta SameSite; __uzmd: falta HttpOnly; __uzmd: falta Secure; __uzmd: falta SameSite; __uzme: falta HttpOnly; __uzme: falta Secure; __uzme: falta SameSite; __uzmf: falta HttpOnly; __uzmf: falta Secure; __uzmf: falta SameSite

- INFO **Cookies detectadas**
  11 cookie(s) encontrada(s)
- INFO **Cookie: nonsession — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: nonsession — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: nonsession — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: s — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: s — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: s — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: ds2 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: ds2 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: ds2 — SameSite**
  SameSite=none
- ALTO **Cookie: ebay — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: ebay — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: ebay — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: __deba — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __deba — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: __deba — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: __uzma — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: __uzma — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: __uzma — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: __uzmb — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: __uzmb — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: __uzmb — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: __uzmc — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: __uzmc — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP

- MEDIO **Cookie: __uzmc — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: __uzmd — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: __uzmd — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: __uzmd — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: __uzme — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: __uzme — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: __uzme — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: __uzmf — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: __uzmf — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: __uzmf — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 (11594 bytes)
- INFO **Reglas robots.txt**
  445 Disallow, 12 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- 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] HTTP a HTTPS redireccion: El servidor no redirige automáticamente el tráfico inseguro al protocolo cifrado, permitiendo conexiones vulnerables.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques XSS y la inyección de contenido malicioso por terceros.
[HIGH] Cookie ds2: Falta el flag HttpOnly, lo que permite que la cookie sea accesible mediante scripts, aumentando el riesgo de robo de sesión.
[HIGH] Cookie ebay: Carece de los atributos HttpOnly y SameSite, exponiendo la sesión a ataques de interceptación y falsificación de peticiones.
[HIGH] Cookies __uzma, __uzmb, __uzmc, __uzmd, __uzme, __uzmf: No cuentan con los flags HttpOnly ni Secure, enviándose de forma insegura y accesible por scripts.
[MEDIUM] Referrer-Policy: La falta de esta cabecera impide controlar qué información de navegación se comparte con otros dominios.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, dejando expuestas funciones como la cámara o el micrófono.
[MEDIUM] Archivos readme.html y README.txt: Estos archivos son accesibles públicamente y podrían revelar información técnica interna de la infraestructura.
[MEDIUM] Cookies nonsession, s, __deba: Falta el atributo SameSite, lo que vuelve al sitio vulnerable a ataques de Cross-Site Request Forgery (CSRF).
[MEDIUM] Robots.txt: El archivo bloquea totalmente el rastreo del sitio mediante la instrucción Disallow, lo cual es una configuración inusual.
[LOW] Server header expuesto: La cabecera revela el uso de ebay-proxy-server, proporcionando pistas a posibles atacantes sobre la tecnología utilizada.