EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.thecommerce.es	Checks	9 pruebas
Dominio	www.thecommerce.es	Hallazgos	58 totales
Fecha	20 de abril de 2026 a las 07:17	Problemas	15 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web ha arrojado una puntuación de 70/100, lo que equivale a una calificación de nota C. Se han ejecutado un total de 9 comprobaciones pasivas, de las cuales 5 resultaron satisfactorias, 2 generaron advertencias y 2 fueron identificadas como fallos críticos. Aunque la implementación del certificado SSL es robusta, existen deficiencias importantes en la configuración de las cabeceras de seguridad y en la protección de las cookies de sesión. Debido a la ausencia de una redirección forzosa a HTTPS y al riesgo de exposición de tokens, se concluye que el sitio es vulnerable ante ataques de interceptación de tráfico y secuestro de sesión.

Resumen de Riesgos

0	6	6	3	43
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 132 dias
Cabeceras de Seguridad	70	AVISO	4/6 presentes. Faltan: X-Frame-Options, Permissi...
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	33	FALLO	PHPSESSID: falta SameSite; xToken: falta HttpOnl...
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 132 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  132 dias restantes (expira: 2026-08-29T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-07-29T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 70/100

Estado: AVISO

4/6 presentes. Faltan: X-Frame-Options, Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: default-src 'self' blob: data: https://arsys.es https://*.arsys.es https://*.pan...
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=600; includeSubDomains;
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: same-origin
- 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=600; includeSubDomains;
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- MEDIO **HSTS max-age**
  max-age=600 (0 dias) — Recomendado minimo 180 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 — 33/100

Estado: FALLO

PHPSESSID: falta SameSite; xToken: falta HttpOnly; xToken: falta SameSite; cookiesEnabled: falta HttpOnly; cookiesEnabled: falta Secure; cookiesEnabled: falta SameSite; xToken: falta HttpOnly; xToken: falta SameSite

- INFO **Cookies detectadas**
  4 cookie(s) encontrada(s)
- INFO **Cookie: PHPSESSID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: PHPSESSID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: xToken — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: xToken — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: xToken — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: cookiesEnabled — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: cookiesEnabled — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: cookiesEnabled — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: xToken — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: xToken — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: xToken — 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 (1196 bytes)
- INFO **Reglas robots.txt**
  19 Disallow, 0 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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 fuerza el uso de conexiones cifradas, permitiendo que la comunicación viaje en texto plano.
[HIGH] X-Frame-Options: La ausencia de esta cabecera permite ataques de clickjacking al no restringir si el sitio puede ser embebido en marcos externos.
[HIGH] Cookie xToken (HttpOnly): La cookie carece del flag HttpOnly, lo que permite que sea accesible mediante scripts del lado del cliente, aumentando el riesgo de robo por XSS.
[HIGH] Cookie cookiesEnabled (HttpOnly/Secure): Esta cookie no tiene atributos de seguridad, permitiendo su acceso vía scripts y su envío a través de conexiones no cifradas.
[MEDIUM] HSTS max-age: La política de seguridad estricta de transporte tiene un tiempo de vida de 0 días, lo que anula su efectividad frente a ataques de degradación de protocolo.
[MEDIUM] Permissions-Policy: No se han definido restricciones sobre qué funciones del navegador (cámara, micrófono, geolocalización) puede ejecutar el sitio.
[MEDIUM] Cookie PHPSESSID (SameSite): La falta del atributo SameSite facilita que la cookie de sesión sea enviada en peticiones de sitios cruzados, exponiendo al usuario a ataques CSRF.
[LOW] Server header expuesto: La cabecera revela el uso de Apache, facilitando a potenciales atacantes la búsqueda de vulnerabilidades específicas para esa tecnología.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a un directorio administrativo, lo que proporciona información valiosa sobre la estructura interna del servidor.
[LOW] sitemap.xml: El archivo de mapa del sitio no fue encontrado, lo que dificulta la auditoría de rutas públicas y la correcta indexación.