EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.copikon.com	Checks	9 pruebas
Dominio	www.copikon.com	Hallazgos	55 totales
Fecha	30 de abril de 2026 a las 12:07	Problemas	20 detectados

D

51/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar una auditoría de seguridad pasiva en el sitio web, se ha obtenido una puntuación de 51/100, lo que equivale a una nota D. Se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 2 generaron advertencias y 3 fueron fallos críticos. El análisis revela deficiencias significativas en la configuración de cabeceras de seguridad y en la gestión de cookies de sesión. Debido a la ausencia de mecanismos de protección esenciales y la falta de redirección forzada a protocolos seguros, se concluye que el sitio es vulnerable y requiere intervención inmediata para proteger la integridad de sus usuarios.

Resumen de Riesgos

0	10	8	2	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 73 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 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	11	FALLO	frontend_lang: falta HttpOnly; frontend_lang: fa...
Contenido Mixto	60	AVISO	2 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 73 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  73 dias restantes (expira: 2026-07-12T07:27:05.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-13T07:27:06.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, 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
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 200 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- 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 — 11/100

Estado: FALLO

frontend_lang: falta HttpOnly; frontend_lang: falta Secure; frontend_lang: falta SameSite; visitor_uuid: falta HttpOnly; visitor_uuid: falta Secure; visitor_uuid: falta SameSite; session_id: falta Secure; session_id: falta SameSite

- INFO **Cookies detectadas**
  3 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
- ALTO **Cookie: visitor_uuid — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: visitor_uuid — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: visitor_uuid — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: session_id — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: session_id — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: session_id — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.odoo.com?utm_source=db&utm_medium=website
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.odoo.com/app/ecommerce?utm_source=db&utm_medi...

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (103 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://www.copikon.com/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] Content-Security-Policy: Falta esta cabecera, lo que deja el sitio expuesto a ataques de Cross-Site Scripting (XSS) e inyección de contenido.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es vulnerable a ataques de Clickjacking, permitiendo que atacantes carguen la web en frames externos maliciosos.
[HIGH] Strict-Transport-Security: La ausencia de HSTS impide que el navegador fuerce conexiones seguras, facilitando ataques de degradación de SSL.
[HIGH] Redirección HTTP a HTTPS: El sitio responde con un código 200 en HTTP en lugar de redirigir a HTTPS, permitiendo comunicaciones no cifradas.
[HIGH] Cookies sin flag Secure: Las cookies frontend_lang, visitor_uuid y session_id se envían en conexiones HTTP, permitiendo su interceptación en ataques Man-in-the-Middle.
[HIGH] Cookies sin flag HttpOnly: Las cookies frontend_lang y visitor_uuid son accesibles mediante scripts del lado del cliente, aumentando el riesgo de robo de identidad en ataques XSS.
[MEDIUM] Cookies sin flag SameSite: Las cookies de sesión no controlan el envío en peticiones de terceros, lo que facilita ataques de Cross-Site Request Forgery (CSRF).
[MEDIUM] Contenido Mixto: Se detectaron dos recursos cargados mediante HTTP dentro de la página HTTPS, lo que debilita la seguridad general del cifrado.
[MEDIUM] Puerto 22 (SSH) abierto: El puerto de acceso remoto está expuesto públicamente, lo que representa un vector de ataque si no está correctamente securizado.
[MEDIUM] Referrer-Policy: Falta la cabecera que controla cuánta información de referencia se envía al navegar desde el sitio.
[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de APIs del navegador como la cámara o el micrófono.
[LOW] Server header expuesto: El servidor revela el uso de Odoo.sh, proporcionando información útil para que un atacante busque vulnerabilidades específicas.
[LOW] Meta generator expuesto: La etiqueta meta confirma el uso de la tecnología Odoo, facilitando el reconocimiento del sistema.