EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://kediem.com	Checks	9 pruebas
Dominio	kediem.com	Hallazgos	45 totales
Fecha	11 de septiembre de 2026 a las 09:16	Problemas	15 detectados

D

50/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del dominio kediem.com ha dado como resultado una puntuación de 50/100, lo que corresponde a una calificación de nota D. Se han ejecutado 9 checks pasivos, de los cuales 4 resultaron exitosos, 1 generó una advertencia y 4 fueron identificados como fallos críticos. La evaluación detectó deficiencias severas en la configuración de cabeceras de seguridad, gestión de sesiones y protocolos de transferencia de archivos. Basándose en estos hallazgos técnicos, se concluye que el sitio es actualmente vulnerable y requiere intervenciones correctivas inmediatas para proteger la integridad de los datos.

Resumen de Riesgos

0	7	5	3	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 87 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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	33	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Same...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 87 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  87 dias restantes (expira: 2026-12-07T03:41:16.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-08T03:41:17.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: LiteSpeed — 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)
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 302 — 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

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 HttpOnly; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: PHPSESSID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: PHPSESSID — 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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] Redirección HTTPS inexistente: El servidor no redirige automáticamente el tráfico HTTP a HTTPS, permitiendo la interceptación de datos.

[HIGH] HSTS (Strict-Transport-Security) ausente: El navegador no es forzado a usar conexiones seguras, permitiendo ataques de degradación de protocolo.
[HIGH] Content-Security-Policy faltante: La ausencia de esta cabecera permite ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options faltante: El sitio es vulnerable a ataques de clickjacking al permitir que el contenido sea embebido en marcos externos.
[HIGH] Puerto 21 (FTP) abierto: El servicio de transferencia de archivos está expuesto y transmite información sin cifrado, facilitando el robo de credenciales.
[HIGH] Cookie PHPSESSID sin HttpOnly: La cookie de sesión es accesible mediante scripts de cliente, aumentando el riesgo de secuestro de sesión vía XSS.
[MEDIUM] X-Content-Type-Options faltante: No se previene el sniffing de tipos MIME, lo que podría permitir la ejecución de archivos maliciosos.
[MEDIUM] Cookie PHPSESSID sin SameSite: La falta de este atributo hace que el sitio sea susceptible a ataques de Cross-Site Request Forgery (CSRF).
[MEDIUM] Puerto 22 (SSH) abierto: El acceso remoto está expuesto, lo que aumenta la superficie de ataque para intentos de intrusión por fuerza bruta.
[MEDIUM] Referrer-Policy faltante: No hay control sobre la información de origen que se envía a otros sitios web.
[MEDIUM] Permissions-Policy faltante: El servidor no restringe el acceso a funciones sensibles del navegador como la cámara o el micrófono.
[LOW] Server header expuesto: El servidor revela que utiliza LiteSpeed, lo que facilita a los atacantes la búsqueda de exploits específicos para esa tecnología.
[LOW] Ausencia de robots.txt y sitemap.xml: El sitio carece de archivos estándar de navegación para rastreadores, afectando la indexación y visibilidad de la estructura.