EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://jkanime.net/	Checks	9 pruebas
Dominio	jkanime.net	Hallazgos	52 totales
Fecha	20 de mayo de 2026 a las 21:34	Problemas	11 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio jkanime.net ha arrojado una puntuación de 72/100, lo que equivale a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias y 1 fue clasificado como fallo crítico. Aunque el cifrado de transporte base es correcto, se han detectado deficiencias importantes en la configuración de cabeceras de seguridad y en la protección de cookies de sesión. Debido a estas omisiones técnicas, el sitio se considera vulnerable ante ataques de interceptación de datos y manipulación de interfaz.

Resumen de Riesgos

0	8	2	1	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 82 dias
Cabeceras de Seguridad	25	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	56	AVISO	XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Se...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 82 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  82 dias restantes (expira: 2026-08-10T16:43:09.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-12T15:43:12.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — 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
- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://jkanime.net/
- 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 — 56/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Secure; jkanime_session: falta Secure; QMdZQdAqWD3MijEO4lvyuPWjvB6TtBMRKjWF6A1Y: falta Secure

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: XSRF-TOKEN — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: jkanime_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: jkanime_session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: jkanime_session — SameSite**
  SameSite=lax
- INFO **Cookie: QMdZQdAqWD3MijEO4lvyuPWjvB6TtBMRKjWF6A1Y — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: QMdZQdAqWD3MijEO4lvyuPWjvB6TtBMRKjWF6A1Y — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: QMdZQdAqWD3MijEO4lvyuPWjvB6TtBMRKjWF6A1Y — 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (24 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **sitemap.xml**
  Presente, ? URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — 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 permite la ejecución de scripts no autorizados, facilitando ataques de Cross-Site Scripting (XSS) e inyección de contenido.
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking, donde un atacante puede cargar la web en un marco invisible para engañar al usuario.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones HTTPS de manera permanente, permitiendo ataques de degradación de protocolo.
[HIGH] Cookie XSRF-TOKEN (CWE-1004): La falta del flag HttpOnly permite que la cookie sea accesible mediante JavaScript, aumentando el riesgo de robo de tokens.
[HIGH] Cookie XSRF-TOKEN (CWE-614): La ausencia del flag Secure provoca que este token sensible pueda ser transmitido a través de conexiones HTTP no cifradas.
[HIGH] Cookie jkanime_session (CWE-614): La cookie de sesión carece del flag Secure, lo que expone la identidad del usuario en redes de comunicación inseguras.
[HIGH] Cookie QMdZQdAqWD3MijEO4lvyuPWjvB6TtBMRKjWF6A1Y (CWE-614): Esta cookie técnica no tiene activado el flag Secure, comprometiendo su integridad en el tránsito.
[MEDIUM] Puerto 8080 (HTTP-Alt): La detección de un puerto alternativo abierto incrementa la superficie de ataque al exponer posibles servicios administrativos o proxies.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso de las APIs del navegador a componentes como la cámara, el micrófono o la geolocalización.
[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando información sobre la infraestructura que puede ser utilizada para dirigir ataques específicos.