EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.inkitt.com/CenizasySombras	Checks	9 pruebas
Dominio	www.inkitt.com	Hallazgos	65 totales
Fecha	4 de junio de 2026 a las 03:26	Problemas	20 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 76/100, obteniendo una nota final de B. Durante el análisis, se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 presentó advertencias y 2 fueron calificados como fallos críticos. Aunque la infraestructura base y el cifrado son robustos, se han detectado debilidades importantes en la configuración de cabeceras y en la protección de cookies de sesión. Se concluye que el sitio es parcialmente vulnerable a ataques de inyección y secuestro de sesión, por lo que requiere ajustes técnicos inmediatos para alcanzar un estado de seguridad óptimo.

Resumen de Riesgos

0	13	6	1	45
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 62 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	ahoy_visitor: falta HttpOnly; ahoy_visitor: falt...
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 62 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  62 dias restantes (expira: 2026-08-05T08:35:09.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-07T07:35:12.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Content-Type-Options, Referrer-Policy, 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
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.inkitt.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS 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**
  React, Next.js

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
- INFO **Archivo /README.txt**
  No accesible (correcto)

- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 33/100

Estado: FALLO

ahoy_visitor: falta HttpOnly; ahoy_visitor: falta Secure; ahoy_visit: falta HttpOnly; ahoy_visit: falta Secure; returning_visitor: falta HttpOnly; returning_visitor: falta Secure; ahoy_visitor_created_at: falta HttpOnly; ahoy_visitor_created_at: falta Secure; ahoy_track: falta HttpOnly; ahoy_track: falta Secure; first_utm_source: falta HttpOnly; first_utm_source: falta Secure

- INFO **Cookies detectadas**
  6 cookie(s) encontrada(s)
- ALTO **Cookie: ahoy_visitor — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: ahoy_visitor — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: ahoy_visitor — SameSite**
  SameSite=lax
- ALTO **Cookie: ahoy_visit — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: ahoy_visit — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: ahoy_visit — SameSite**
  SameSite=lax
- ALTO **Cookie: returning_visitor — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: returning_visitor — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: returning_visitor — SameSite**
  SameSite=lax
- ALTO **Cookie: ahoy_visitor_created_at — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: ahoy_visitor_created_at — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: ahoy_visitor_created_at — SameSite**
  SameSite=lax
- ALTO **Cookie: ahoy_track — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: ahoy_track — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: ahoy_track — SameSite**
  SameSite=lax
- ALTO **Cookie: first_utm_source — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: first_utm_source — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: first_utm_source — 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 (1156 bytes)
- INFO **Reglas robots.txt**
  6 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://www.inkitt.com/sitemaps/main_sitemap.xml
- 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] Cookies sin flags de seguridad: Las cookies ahoy_visitor, ahoy_visit, returning_visitor, ahoy_visitor_created_at, ahoy_track y first_utm_source carecen de los atributos HttpOnly y Secure, lo que permite su robo mediante scripts maliciosos o interceptación en conexiones no cifradas.
[HIGH] Content-Security-Policy faltante: La ausencia de esta cabecera impide definir qué fuentes de contenido son confiables, dejando el sitio expuesto a ataques de Cross-Site Scripting (XSS) e inyección de datos.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de un puerto alternativo de servidor web o proxy aumenta la superficie de ataque y puede revelar servicios no protegidos.
[MEDIUM] Panel de administración expuesto: La ruta /administrator/ es accesible públicamente, lo que facilita intentos de acceso no autorizado mediante fuerza bruta.
[MEDIUM] Archivo readme.html accesible: La presencia de este archivo en la raíz puede exponer información técnica sobre la plataforma o versiones de software subyacente.
[MEDIUM] X-Content-Type-Options faltante: El navegador podría intentar interpretar el contenido de forma distinta al tipo MIME declarado, facilitando ataques de sniffing.
[MEDIUM] Referrer-Policy faltante: No existe control sobre la información de procedencia que se envía a otros sitios al hacer clic en enlaces salientes.
[MEDIUM] Permissions-Policy faltante: El sitio no restringe el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando información útil a un atacante para buscar vulnerabilidades específicas de la plataforma.