

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://kissu.com.ec/	Checks	9 pruebas
Dominio	kissu.com.ec	Hallazgos	44 totales
Fecha	9 de abril de 2026 a las 10:21	Problemas	6 detectados

B

87/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio kissu.com.ec ha dado como resultado una puntuación de 87/100, lo que equivale a una nota B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 fue calificado como fallo. Aunque el cifrado de datos es excelente, la ausencia de ciertas cabeceras de seguridad y la exposición de puertos adicionales representan un riesgo moderado. Se concluye que el sitio es generalmente seguro, pero presenta vulnerabilidades técnicas que deben ser mitigadas para prevenir ataques de inyección.

Resumen de Riesgos

0 CRITICO	1 ALTO	2 MEDIO	3 BAJO	38 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 82 dias
Cabeceras de Seguridad	75	AVISO	5/6 presentes. Faltan: Content-Security-Policy
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	100	OK	No se encontraron cookies
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	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: 2026-06-30T02:00:20.000Z)
- INFO Fecha de emision
Emitido desde: 2026-04-01T01:03:40.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

5/6 presentes. Faltan: Content-Security-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=7776000
- INFO

X-Content-Type-Options
Presente: nosniff
- INFO

Referrer-Policy
Presente: same-origin
- INFO

Permissions-Policy
Presente: accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-write=...

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://kissu.com.ec/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=7776000
- BAJO

HSTS includeSubDomains
HSTS no cubre subdominios
- MEDIO

HSTS max-age
max-age=7776000 (90 dias) — Recomendado minimo 180 dias
- INFO

Respuesta HTTPS
HTTPS responde con status 403

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 — 100/100

Estado: OK

No se encontraron cookies

- INFO

Cookies detectadas
El sitio no establece cookies en la respuesta inicial

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 403)
- BAJO

sitemap.xml
No encontrado (HTTP 403)
- 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 ataques Cross-Site Scripting (XSS) y la inyección de contenido malicioso.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó este puerto abierto, el cual suele utilizarse para servicios secundarios o paneles de administración que podrían ser explotados.

[MEDIUM] HSTS max-age: La configuración actual de 90 días es inferior al estándar recomendado de 180 días para garantizar una conexión cifrada persistente.

[LOW] Server header expuesto: El encabezado revela el uso de Cloudflare, proporcionando información técnica que un atacante puede usar para perfilar la infraestructura.

[LOW] robots.txt y sitemap.xml: El servidor deniega el acceso a estos archivos con un error 403, lo que impide una correcta auditoría de la estructura del sitio.