EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ruwark.cloud/	Checks	9 pruebas
Dominio	ruwark.cloud	Hallazgos	44 totales
Fecha	25 de septiembre de 2026 a las 15:41	Problemas	11 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado sobre el dominio evaluado arrojo una puntuacion final de 73/100, lo que equivale a una nota de C. Durante la evaluacion se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, mientras que se registraron 2 advertencias y 2 fallos criticos en la configuracion del servidor. El sitio presenta una base solida en cuanto a cifrado de conexion, pero carece de cabeceras de proteccion fundamentales para mitigar ataques comunes en el navegador. Aunque no se detectaron vulnerabilidades de ejecucion inmediata, la ausencia de politicas de seguridad estrictas situa al sitio en un estado vulnerable frente a ataques de intermediario y clickjacking. Se concluye que el sitio requiere ajustes tecnicos urgentes para mejorar su postura de seguridad actual y alcanzar un nivel de proteccion profesional.

Resumen de Riesgos

0	3	4	4	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 68 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
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	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 68 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  68 dias restantes (expira: 2026-12-02T07:20:03.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-03T07:20:04.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor
- BAJO **X-Powered-By expuesto**
  X-Powered-By: Next.js — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://www....
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://ruwark.cloud/
- 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
- INFO **Tecnologias detectadas**
  Next.js, 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 — 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 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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] X-Frame-Options: Falta esta cabecera en el servidor, lo que permite que el sitio sea cargado dentro de iframes y facilita ataques de clickjacking para engañar a los usuarios.

[HIGH] Strict-Transport-Security: La ausencia de HSTS impide que el navegador fuerce conexiones cifradas permanentemente, dejando la comunicacion expuesta a ataques de degradacion de protocolo.
[MEDIUM] Puerto 8080 (HTTP-Alt): El puerto 8080 se encuentra abierto, lo que representa una superficie de ataque adicional al exponer un servidor web alternativo o un proxy que podria no estar debidamente protegido.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que podria llevar al navegador a interpretar archivos de forma incorrecta y ejecutar scripts maliciosos.
[MEDIUM] Referrer-Policy: No se controla la informacion de referencia enviada a otros sitios, lo que podria filtrar rutas internas o parametros de navegacion a terceros.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la camara o el microfono, aumentando el riesgo en caso de una inyeccion de codigo.
[LOW] Server header expuesto: El servidor revela explicitamente el uso de Cloudflare, facilitando a un atacante potencial el reconocimiento de la infraestructura utilizada.
[LOW] X-Powered-By expuesto: Se detecto el uso del framework Next.js, lo que permite a actores malintencionados dirigir ataques especificos contra vulnerabilidades conocidas de dicha tecnologia.
[LOW] robots.txt y sitemap.xml: La ausencia de estos archivos genera errores 404 y dificulta la correcta indexacion y el control de acceso de rastreadores externos.