EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://runachay.runacode.com	Checks	9 pruebas
Dominio	runachay.runacode.com	Hallazgos	45 totales
Fecha	19 de junio de 2026 a las 20:27	Problemas	8 detectados

B

77/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado a la plataforma arroja una puntuación de 77/100, lo que resulta en una nota de calificación B. Durante la auditoría se ejecutaron 9 comprobaciones pasivas, obteniendo 5 resultados satisfactorios, 3 advertencias y 1 fallo crítico relacionado con la configuración del servidor. El sitio web demuestra una base sólida en cuanto a cifrado de datos y redirecciones seguras, pero presenta debilidades estructurales en sus políticas de seguridad del lado del cliente. En su estado actual, el sitio se considera moderadamente seguro, aunque vulnerable a ataques de inyección y manipulación de interfaz por falta de cabeceras defensivas.

Resumen de Riesgos

0	2	4	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 73 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	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 73 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  73 dias restantes (expira: 2026-08-31T09:16:22.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-02T08:16:27.000Z
- 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-Frame-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
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://runachay.runacode.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 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

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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://runachay.com/

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (85 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- 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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados, facilitando ataques de XSS e inyección de contenido malicioso.

[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking, donde un atacante puede cargar la web en un marco invisible para engañar al usuario.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó un puerto alternativo abierto que podría exponer servicios administrativos o proxies no protegidos adecuadamente.
[MEDIUM] Contenido Mixto: La referencia al recurso http://runachay.com/ mediante una conexión no cifrada debilita la integridad de la sesión HTTPS global.
[MEDIUM] Referrer-Policy: La falta de esta política puede provocar la filtración involuntaria de información sensible en las URLs de origen hacia sitios externos.
[MEDIUM] Permissions-Policy: El navegador no tiene restricciones para acceder a APIs del sistema, como la cámara o el micrófono, lo que supone un riesgo potencial de privacidad.
[LOW] Server header expuesto: El servidor revela el uso de tecnología Cloudflare, lo que facilita a un atacante potencial el reconocimiento de la infraestructura.
[LOW] sitemap.xml: La ausencia de este archivo dificulta la auditoría de contenidos y la correcta indexación de la estructura del sitio.