EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.monederoqr.com/acceso-corporativo	Checks	9 pruebas
Dominio	www.monederoqr.com	Hallazgos	51 totales
Fecha	5 de junio de 2026 a las 01:10	Problemas	11 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web determinó una puntuación de 73/100, lo que equivale a una calificación de grado C. Durante la auditoría se ejecutaron 9 checks pasivos, resultando en 6 verificaciones satisfactorias, 1 advertencia y 2 fallos críticos en la configuración. Aunque la infraestructura base presenta fortalezas en el cifrado de conexión, la ausencia de cabeceras de seguridad y la gestión deficiente de cookies representan riesgos significativos. En su estado actual, el sitio se considera vulnerable a ataques de inyección y secuestro de sesiones.

Resumen de Riesgos

0	4	5	2	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 77 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	CMS detectado: Wix
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	0	FALLO	ssr-caching: falta HttpOnly; ssr-caching: falta ...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 77 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  77 dias restantes (expira: 2026-08-21T10:22:26.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-23T10:22:27.000Z
- 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: Pepyaka — 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=31556952
- 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://www.monederoqr.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31556952
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31556952 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Wix

- 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**
  Detectado via HTML body
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Wix.com Website Builder
- INFO **Tecnologias detectadas**
  React, 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 — 0/100

Estado: FALLO

ssr-caching: falta HttpOnly; ssr-caching: falta Secure; ssr-caching: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: ssr-caching — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: ssr-caching — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: ssr-caching — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://creditrune.servihome.com.mx/nosotros.html#

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (492 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://www.monederoqr.com/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- INFO **Puerto 8080 (HTTP-Alt)**
  Cerrado — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: Falta — La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] X-Frame-Options: Falta — El sitio es vulnerable a ataques de clickjacking, permitiendo que atacantes carguen la web en marcos invisibles para engañar al usuario.
[HIGH] Cookie ssr-caching (HttpOnly): Falta — La cookie es accesible mediante JavaScript, lo que facilita el robo de sesiones en caso de una vulnerabilidad de scripts.
[HIGH] Cookie ssr-caching (Secure): Falta — La información de sesión se transmite sin el atributo de seguridad, pudiendo ser interceptada en conexiones no cifradas.
[MEDIUM] Cookie ssr-caching (SameSite): Falta — El sitio no restringe el envío de cookies en solicitudes de origen cruzado, aumentando el riesgo de ataques CSRF.
[MEDIUM] Contenido Mixto: Se detectó un recurso externo (hoja de estilo) cargado mediante HTTP en una página HTTPS, rompiendo la integridad de la conexión.
[MEDIUM] Referrer-Policy: Falta — No se controla qué información de navegación se envía a terceros al seguir enlaces externos.
[MEDIUM] Permissions-Policy: Falta — No existen restricciones sobre el acceso de las APIs del navegador a funciones sensibles como cámara o micrófono.
[MEDIUM] Robots.txt (Bloqueo total): El archivo impide el rastreo completo del sitio mediante la directiva Disallow, lo que puede afectar la visibilidad y auditoría.
[LOW] Server header expuesto: El servidor revela el software Pepyaka, facilitando la búsqueda de exploits específicos para esa tecnología.
[LOW] Meta generator expuesto: Se detectó el uso de Wix.com Website Builder, exponiendo información sobre la plataforma de desarrollo.