EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://corporate.monederoqr.com/Creditrune/Login.aspx	Checks	9 pruebas
Dominio	corporate.monederoqr.com	Hallazgos	18 totales
Fecha	5 de junio de 2026 a las 01:09	Problemas	3 detectados

F

37/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al portal arroja una puntuación crítica de 37/100, lo que conlleva una calificación de nota F. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales solo uno resultó satisfactorio, mientras que se identificaron fallos graves en el cifrado y múltiples errores de configuración. La ausencia de un certificado SSL válido y la incapacidad de verificar cabeceras de seguridad básicas representan un riesgo extremo para la integridad de los datos. Se concluye que el sitio es actualmente vulnerable y no es apto para el manejo de información sensible o transaccional.

Resumen de Riesgos

1	0	0	2	15
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: FALLO

Certificado SSL no valido

- CRITICO **Certificado valido**
  El certificado SSL NO es valido
- INFO **Dias hasta expiracion**
  102 dias restantes (expira: 2026-09-14T20:21:40.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-08-13T20:21:40.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  Error al acceder

- BAJO **sitemap.xml**
  Error al acceder

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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

[CRÍTICA] Certificado SSL no válido: El sitio carece de un certificado digital funcional, lo que impide el cifrado de la conexión y permite la interceptación de datos.
[ALTA] Cabeceras de seguridad faltantes: No se detectaron protecciones contra ataques de inyección de código, Clickjacking o XSS, dejando el navegador del usuario desprotegido.
[ALTA] Fallo en redirección HTTPS: El sitio no fuerza una conexión segura, permitiendo que las comunicaciones viajen de forma legible a través de la red.
[MEDIA] Seguridad de cookies no verificada: Al no detectarse atributos de seguridad en las cookies, las sesiones de los usuarios podrían ser secuestradas por atacantes.
[BAJA] Ausencia de robots.txt y sitemap.xml: El servidor no cuenta con archivos de guía para rastreadores, lo que indica una configuración de servidor web incompleta o deficiente.