EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.rifavo.com/?fbclid=IwcGRvZgNleHRuA2FlbQIxMQBzcnRjBmFwcF9pZA8yMzUyNTI5Q2OTI1OTgyNzkAAR4z67Vi1vkAkXA5am1qzp7pBCwmUnCzAqDs_zlxiQ12-5FuZ-jaBWWsgHCUPw_aem_MEDYkn_yxmf9bThewXs66Q	Duración	9 minutos
Dominio	www.rifavo.com	Hallazgos	49 totales
Fecha	17 de agosto de 2026 a las 18:35	Problemas	10 detectados

B

84/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja una puntuación de 84/100 con una calificación de grado B. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 8 resultaron satisfactorias y 1 presentó fallos significativos en la configuración de seguridad. Aunque el cifrado de datos y la gestión de certificados son excelentes, el portal carece de protecciones esenciales a nivel de cabeceras HTTP. En conclusión, el sitio se considera moderadamente seguro, pero presenta vulnerabilidades configurativas que podrían ser explotadas para ataques de inyección o suplantación.

Resumen de Riesgos

0	2	7	1	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 86 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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	100	OK	No se detecto contenido mixto
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 86 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  86 dias restantes (expira: 2026-11-12T02:29:35.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-14T02:29:36.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: Vercel — 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
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 308 redirige a https://www.rifavo.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000
- BAJO **HSTS includeSubDomains**
  HSTS no 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
- INFO **Tecnologias detectadas**
  React

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (852 bytes)
- INFO **Reglas robots.txt**
  5 Disallow, 17 Allow
- INFO **Sitemap en robots.txt**
  https://www.rifavo.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 esta cabecera que es vital para prevenir ataques de Cross-Site Scripting (XSS) e inyecciones de contenido malicioso.
[HIGH] X-Frame-Options: La ausencia de esta instrucción permite que el sitio sea cargado dentro de marcos de otras webs, facilitando ataques de clickjacking.
[MEDIUM] X-Content-Type-Options: No se previene el sniffing de tipos MIME, lo que podría permitir al navegador ejecutar archivos con formatos incorrectos y peligrosos.
[MEDIUM] Referrer-Policy: La falta de esta política impide controlar qué información de navegación se comparte con otros dominios al seguir enlaces.
[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador, permitiendo potencialmente el acceso no autorizado a APIs como la cámara o el micrófono.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y puede ser utilizado por atacantes para obtener información técnica sobre la plataforma.
[MEDIUM] Rutas de login expuestas: Se detectaron paneles de acceso en /wp-login.php, /administrator/ y /user/login abiertos a cualquier usuario de internet.
[LOW] Server header expuesto: El encabezado revela explícitamente el uso de Vercel, proporcionando información sobre la infraestructura tecnológica subyacente.