EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://arrozimperio.net/	Checks	9 pruebas
Dominio	arrozimperio.net	Hallazgos	48 totales
Fecha	8 de mayo de 2026 a las 18:21	Problemas	10 detectados

B

89/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web arrozimperio.net ha resultado en una puntuación de 89/100 con una nota de B. Se ejecutaron un total de 9 checks pasivos, de los cuales 8 resultaron satisfactorios y uno se identificó como fallo debido a deficiencias en las cabeceras de respuesta. El cifrado de datos y las redirecciones de transporte seguro funcionan correctamente, proporcionando una base de protección sólida. No obstante, la exposición de rutas administrativas y la ausencia de políticas de seguridad en el navegador elevan el riesgo de ataques dirigidos. En conclusión, el sitio es mayormente seguro pero presenta vulnerabilidades configurativas que deben ser mitigadas.

Resumen de Riesgos

0	2	7	1	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 102 dias
Cabeceras de Seguridad	45	FALLO	Solo 3/6 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 102 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  102 dias restantes (expira: 2026-08-18T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-18T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 45/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Permissions-Policy

- 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=10886400; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: same-origin
- 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://arrozimperio.net/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=10886400; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- MEDIO **HSTS max-age**
  max-age=10886400 (126 dias) — Recomendado minimo 180 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

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- 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 (246 bytes)
- INFO **Reglas robots.txt**
  7 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://arrozimperio.net/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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

[ALTA] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados y ataques de inyección de contenido XSS.
[ALTA] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking donde un atacante puede superponer la web en un marco invisible.
[MEDIA] Permissions-Policy: Falta de restricciones sobre el uso de APIs del navegador como la cámara o el micrófono por parte de terceros.
[MEDIA] Rutas de administración expuestas: Los endpoints /wp-login.php, /administrator/ y /user/login son accesibles, lo que facilita intentos de acceso no autorizado.
[MEDIA] Archivos técnicos accesibles: La disponibilidad pública de /readme.html y /README.txt puede revelar detalles de la infraestructura a atacantes.
[MEDIA] Configuración de HSTS: El tiempo de persistencia de la política de seguridad es de 126 días, por debajo del estándar recomendado de 180 días.
[BAJA] Exposición en robots.txt: La mención de rutas con el término admin en el archivo de indexación facilita el reconocimiento de directorios sensibles.