

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://tms.ripley.com.pe/login
Dominio tms.ripley.com.pe
Fecha 7 de octubre de 2026 a las 21:44

Checks 9 pruebas
Hallazgos 45 totales
Problemas 7 detectados

C

73/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 73/100 y una nota C. Durante la evaluación se ejecutaron un total de 9 controles pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fallos críticos. Aunque la plataforma utiliza un cifrado SSL sólido, presenta carencias importantes en la implementación de políticas de transporte seguro y gestión de servidores. Debido a la falta de redirecciones automáticas y cabeceras de protección, el sitio se considera actualmente vulnerable ante ataques de interceptación de tráfico y reconocimiento de infraestructura. Se recomienda una intervención técnica inmediata para mejorar la postura de seguridad global.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 42 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	1 cookies, todas con flags correctos
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 42 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
42 dias restantes (expira: 2026-11-19T04:40:22.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-21T03:40:37.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

- BAJO Server header expuesto
Server: cloudflare — Revela tecnologia del servidor

- INFO

Content-Security-Policy
Presente: default-src 'none'; script-src 'nonce-CnorvY0KdUnRKmOtjXXrli' 'unsafe-eval' http...
- INFO

X-Frame-Options
Presente: SAMEORIGIN
- ALTO

Strict-Transport-Security
Falta — Fuerza conexiones HTTPS (HSTS)
- INFO

X-Content-Type-Options
Presente: nosniiff
- INFO

Referrer-Policy
Presente: same-origin
- INFO

Permissions-Policy
Presente: accelerometer=(),camera=(),clipboard-read=(),clipboard-write=(),geolocation=(),g...

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO

HTTP !' HTTPS redireccion
HTTP 403 — No redirige a HTTPS
- ALTO

HSTS (Strict-Transport-Security)
HSTS no configurado — El navegador no fuerza HTTPS
- INFO

Respuesta HTTPS
HTTPS responde con status 403

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

1 cookies, todas con flags correctos

- INFO

Cookies detectadas
1 cookie(s) encontrada(s)
- INFO

Cookie: __cf_bm — HttpOnly
HttpOnly activo — No accesible via JavaScript
- INFO

Cookie: __cf_bm — Secure
Flag Secure activo — Solo se envia por HTTPS
- INFO

Cookie: __cf_bm — SameSite
SameSite=none

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO

robots.txt
No encontrado (HTTP 403)
- BAJO

sitemap.xml
No encontrado (HTTP 403)
- 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] Strict-Transport-Security: Falta esta cabecera esencial que instruye al navegador a comunicarse exclusivamente mediante HTTPS para prevenir ataques de degradación.

[HIGH] HTTP a HTTPS redirección: El servidor no redirige el tráfico inseguro al puerto seguro, respondiendo con un error 403 en lugar de forzar el cifrado.

[MEDIUM] Puerto 8080 (HTTP-Alt) ABIERTO: La exposición de puertos alternativos aumenta la superficie de ataque y puede revelar servicios administrativos no protegidos.

[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando información valiosa a posibles atacantes sobre la tecnología de red utilizada.

[LOW] robots.txt no encontrado: La ausencia de este archivo o su bloqueo impide la gestión correcta de la indexación por parte de motores de búsqueda.

[LOW] sitemap.xml no encontrado: No se detectó un mapa del sitio accesible, lo que dificulta la auditoría de la estructura lógica del portal.