EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Rediplays.com	Checks	9 pruebas
Dominio	rediplays.com	Hallazgos	52 totales
Fecha	10 de mayo de 2026 a las 20:41	Problemas	6 detectados

A

92/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado a Rediplays.com arroja una puntuación de 92/100, lo que equivale a una calificación de nota A. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 generaron advertencias, sin detectarse fallos críticos de seguridad. Los resultados indican una implementación sólida de protocolos de cifrado y cabeceras defensivas. En conclusión, el sitio se considera seguro, aunque presenta vectores de riesgo menores relacionados con la exposición de información y configuración de cookies que deben ser subsanados.

Resumen de Riesgos

0	1	4	1	46
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 84 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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	83	AVISO	XSRF-TOKEN: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 84 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  84 dias restantes (expira: 2026-08-02T10:46:09.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-04T10:46:10.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

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

- INFO **Content-Security-Policy**
  Presente: default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline' https:; styl...
- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), micr...

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://rediplays.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 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**
  Next.js

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 /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 83/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: rediplays_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: rediplays_session — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: rediplays_session — SameSite**
  SameSite=lax

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (66 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 0 Allow
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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] Cookie XSRF-TOKEN: La ausencia del atributo HttpOnly permite que la cookie sea accesible mediante scripts del lado del cliente, aumentando significativamente el riesgo de ataques de Cross-Site Scripting (XSS).
[MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto y expone un servidor web alternativo o proxy, lo que incrementa la superficie de ataque disponible.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y puede ser utilizado por atacantes para obtener detalles técnicos sobre la estructura interna del sitio.
[MEDIUM] Archivo /README.txt: La exposición de este documento permite la lectura de información técnica que debería ser privada.
[MEDIUM] Ruta /user/login: El panel de inicio de sesión es accesible para cualquier usuario de internet, facilitando posibles ataques de fuerza bruta dirigidos.
[LOW] Cabecera Server expuesta: El servidor revela el uso de Cloudflare, proporcionando información sobre la infraestructura tecnológica que podría ser aprovechada en una fase de reconocimiento.