EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://polideportivoarcoiris.weebly.com/	Checks	9 pruebas
Dominio	polideportivoarcoiris.weebly.com	Hallazgos	47 totales
Fecha	25 de abril de 2026 a las 20:46	Problemas	11 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio polideportivoarcoiris.weebly.com arroja una puntuación de 68/100, lo que equivale a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias y 1 fue identificado como fallo crítico. Aunque el sitio cuenta con un certificado SSL vigente, presenta carencias importantes en la implementación de cabeceras de seguridad y protección contra ataques de inyección. La exposición de puertos no estándar y la falta de políticas de transporte estricto elevan el riesgo operativo. En su estado actual, el sitio se considera vulnerable ante ataques de intermediarios y secuestro de clics.

Resumen de Riesgos

0	4	6	1	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 77 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	67	AVISO	__cf_bm: falta SameSite
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 77 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  77 dias restantes (expira: 2026-07-11T21:03:56.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-12T21:03:57.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — 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
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://polideportivoarcoiris.weebly.com/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- 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

- 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 — 67/100

Estado: AVISO

__cf_bm: falta SameSite

- 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
- MEDIO **Cookie: __cf_bm — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 (181 bytes)
- INFO **Reglas robots.txt**
  3 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://polideportivoarcoiris.weebly.com/sitemap.xml
- 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] Content-Security-Policy faltante: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso en el navegador del usuario.
[HIGH] X-Frame-Options faltante: El sitio no previene ser cargado dentro de un frame, lo que lo hace vulnerable a ataques de clickjacking para engañar a los visitantes.
[HIGH] Strict-Transport-Security (HSTS) faltante: No se obliga a los navegadores a usar exclusivamente conexiones HTTPS, permitiendo ataques de degradación de protocolo.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: Se detectó un puerto alternativo accesible que podría ser utilizado para servicios no protegidos o proxies.
[MEDIUM] Cookie __cf_bm sin atributo SameSite: La falta de esta configuración en las cookies de Cloudflare incrementa el riesgo de ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] X-Content-Type-Options faltante: El sitio es vulnerable al sniffing de tipos MIME, lo que podría permitir que archivos de texto sean interpretados como scripts ejecutables.
[MEDIUM] Referrer-Policy faltante: No se controla qué información de procedencia se envía a terceros, pudiendo comprometer la privacidad de la navegación.
[MEDIUM] Permissions-Policy faltante: No se restringe el acceso de las APIs del navegador a componentes sensibles como la cámara o el micrófono.
[MEDIUM] Bloqueo total en robots.txt: El archivo de configuración bloquea la indexación de todo el sitio, lo que suele ser un error de configuración o una medida de ocultación ineficiente.
[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando información técnica que ayuda a un atacante a perfilar el objetivo.