EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://link.factorstudios.io/Aitq	Checks	9 pruebas
Dominio	link.factorstudios.io	Hallazgos	50 totales
Fecha	23 de julio de 2026 a las 17:22	Problemas	5 detectados

A

91/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado ha otorgado una puntuación de 91/100 y una nota A al sitio web analizado. Durante el proceso se ejecutaron 9 comprobaciones pasivas, obteniendo 6 resultados satisfactorios y 3 advertencias, sin registrarse fallos críticos. Aunque no se realizó un pentest activo, los datos recolectados indican una postura de seguridad sólida con una excelente gestión de certificados. Se concluye que el sitio es seguro para el uso general, siempre que se subsanen las deficiencias menores detectadas en las cabeceras y la protección de cookies. La implementación de protocolos de cifrado modernos garantiza un entorno confiable para el intercambio de información.

Resumen de Riesgos

0	2	3	0	45
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 73 dias
Cabeceras de Seguridad	75	AVISO	4/6 presentes. Faltan: X-Frame-Options, Referrer...
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	wa_lang_pref: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 73 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  73 dias restantes (expira: 2026-10-04T07:01:33.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-06T07:01:34.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

4/6 presentes. Faltan: X-Frame-Options, Referrer-Policy

- INFO **Content-Security-Policy**
  Presente: default-src 'self' blob:;script-src 'nonce-v9GLS5Rl' *.facebook.com *.fbcdn.net ...

- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; preload; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- INFO **Permissions-Policy**
  Presente: accelerometer=(), attribution-reporting=(), autoplay=(), bluetooth=(), camera=()...

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://link.factorstudios.io/
- 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
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 83/100

Estado: AVISO

wa_lang_pref: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: wa_lang_pref — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: wa_lang_pref — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: wa_lang_pref — SameSite**
  SameSite=lax
- INFO **Cookie: wa_ul — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: wa_ul — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: wa_ul — 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 (23 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 1 Allow
- 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

[HIGH] X-Frame-Options: La ausencia de esta cabecera de seguridad permite que el sitio sea cargado en marcos (iframes), lo que facilita ataques de clickjacking para engañar a los usuarios.
[HIGH] Cookie wa_lang_pref: Esta cookie carece del atributo HttpOnly, lo que la hace accesible mediante scripts del lado del cliente y aumenta el riesgo de robo de sesión mediante ataques XSS.
[MEDIUM] Referrer-Policy: La falta de esta directiva impide controlar cuánta información de procedencia se envía a otros dominios al navegar por enlaces externos.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y suele contener información técnica que ayuda a potenciales atacantes a reconocer la infraestructura del servidor.
[MEDIUM] Archivo /README.txt: El acceso público a este documento puede revelar detalles internos del desarrollo o configuraciones de herramientas que no deberían ser visibles.