EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://freewillex.com	Checks	9 pruebas
Dominio	freewillex.com	Hallazgos	48 totales
Fecha	9 de mayo de 2026 a las 18:06	Problemas	13 detectados

B

81/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web freewillex.com ha arrojado una puntuación de 81/100, lo que otorga una nota B en la escala de cumplimiento. Se ejecutaron un total de 9 comprobaciones pasivas, obteniendo 6 resultados satisfactorios, 2 advertencias por configuraciones mejorables y 1 fallo crítico en la seguridad del servidor. La plataforma demuestra una gestión robusta del cifrado y la identidad mediante SSL/TLS, pero presenta deficiencias notables en la implementación de cabeceras de seguridad defensivas. Aunque el transporte de datos es íntegro, la exposición de puertos adicionales y la falta de políticas contra inyección de código sugieren que el sitio es moderadamente seguro, pero presenta vectores de ataque explotables. Se concluye que el sitio web es funcionalmente seguro para el tráfico estándar, pero vulnerable ante ataques dirigidos a la capa de aplicación y de interfaz.

Resumen de Riesgos

0	2	10	1	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 49 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 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	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 49 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  49 dias restantes (expira: 2026-06-27T20:52:47.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-29T19:53:56.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-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
- INFO **Strict-Transport-Security**
  Presente: max-age=0; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- 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://freewillex.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=0; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- MEDIO **HSTS max-age**
  max-age=0 (0 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (11901 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- 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] Content-Security-Policy: Falta esta cabecera crítica, lo que deja al sitio expuesto a ataques de Cross-Site Scripting (XSS) y ataques de inyección de datos.
[HIGH] X-Frame-Options: La ausencia de esta política permite que el sitio sea embebido en marcos externos, facilitando ataques de secuestro de clics o clickjacking.
[MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto y accesible, lo que aumenta la superficie de exposición ante posibles servicios mal configurados o proxies.
[MEDIUM] HSTS max-age: La política de transporte estricto está configurada con un valor de 0 días, invalidando la protección recomendada contra ataques de degradación de protocolo.
[MEDIUM] Referrer-Policy: No existe una política para controlar la información de origen que se comparte con terceros al navegar por el sitio.
[MEDIUM] Permissions-Policy: No se han definido restricciones para las APIs del navegador, permitiendo potencialmente el acceso a periféricos como cámara o micrófono.
[MEDIUM] Rutas administrativas expuestas: Se detectaron paneles de acceso público en /wp-login.php, /administrator/ y /user/login, lo que facilita intentos de fuerza bruta.
[MEDIUM] Archivos informativos accesibles: Los archivos /readme.html y /README.txt están expuestos, pudiendo filtrar información técnica sobre la infraestructura interna.
[MEDIUM] Robots.txt restrictivo: El archivo bloquea la indexación de todo el contenido mediante la directiva Disallow: /, lo que podría ocultar estructuras pero también indicar configuraciones erróneas.
[LOW] Server header expuesto: El encabezado del servidor revela el uso de Cloudflare, proporcionando información útil a atacantes durante la fase de reconocimiento.