EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://devkiper.com/	Checks	9 pruebas
Dominio	devkiper.com	Hallazgos	52 totales
Fecha	28 de abril de 2026 a las 23:43	Problemas	6 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web ha arrojado una puntuación de 85/100, lo que equivale a una calificación de grado B. Durante la auditoría se ejecutaron 9 checks pasivos, resultando en 6 verificaciones exitosas, 2 advertencias y 1 fallo crítico en la configuración de cabeceras. Aunque la base de cifrado es robusta, se identificaron carencias en la protección contra ataques de suplantación y manejo de sesiones. Debido a la ausencia de cabeceras de seguridad esenciales y la exposición de puertos alternativos, se concluye que el sitio es parcialmente vulnerable a ataques dirigidos.

Resumen de Riesgos

0	2	3	1	46
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 44 dias
Cabeceras de Seguridad	55	FALLO	Solo 3/6 presentes. Faltan: X-Frame-Options, X-C...
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	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 44 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  44 dias restantes (expira: 2026-06-12T09:57:58.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-14T09:00:41.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: FALLO

Solo 3/6 presentes. Faltan: X-Frame-Options, X-Content-Type-Options, Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: frame-ancestors 'self' http://webvisor.com https://webvisor.com metrika.yandex.r...
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=15724800; includeSubDomains
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- 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://devkiper.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15724800; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=15724800 (182 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 429

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

- 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 — 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: uteach_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: uteach_session — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: uteach_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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (52 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 0 Allow
- INFO **sitemap.xml**
  Presente, 10 URLs
- 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] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea embebido en marcos de otras páginas, facilitando ataques de clickjacking para engañar a los usuarios.
[HIGH] Cookie XSRF-TOKEN: Esta cookie carece del atributo HttpOnly, lo que permite que sea accesible a través de scripts de JavaScript y aumenta significativamente el riesgo de robo de sesión mediante XSS.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador puede intentar interpretar el contenido de los archivos de forma distinta a la declarada, permitiendo la ejecución de código malicioso.
[MEDIUM] Permissions-Policy: La falta de esta directiva impide restringir el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó este puerto abierto, el cual suele utilizarse para servicios de administración o proxies, ampliando innecesariamente la superficie de ataque.
[LOW] Cabecera Server expuesta: El servidor revela el uso de la tecnología Cloudflare, lo que proporciona información técnica que un atacante podría utilizar para planificar vectores de ataque específicos.