EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://user.aiminers.net/user/dashboard	Checks	9 pruebas
Dominio	user.aiminers.net	Hallazgos	48 totales
Fecha	3 de mayo de 2026 a las 22:55	Problemas	13 detectados

C

66/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 66/100, lo que equivale a una nota de C. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, se generó 1 advertencia y se identificaron 3 fallos críticos. Aunque la infraestructura de red básica cumple con ciertos estándares, la configuración de la aplicación web presenta deficiencias importantes en la protección de datos y cabeceras. Por lo tanto, se concluye que el sitio es actualmente vulnerable a ataques de secuestro de sesión y ataques de inyección.

Resumen de Riesgos

0	7	5	1	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 65 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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
Seguridad de Cookies	33	FALLO	googtrans: falta HttpOnly; googtrans: falta Secu...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 65 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  65 dias restantes (expira: 2026-07-08T08:32:40.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-09T07:35:17.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, 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
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://user.aiminers.net/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no 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

Seguridad de Cookies — 33/100

Estado: FALLO

googtrans: falta HttpOnly; googtrans: falta Secure; googtrans: falta SameSite; XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Secure; laravel_session: falta Secure

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- ALTO **Cookie: googtrans — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: googtrans — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: googtrans — SameSite**
  Falta SameSite — Vulnerable a CSRF

- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: XSRF-TOKEN — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: laravel_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: laravel_session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: laravel_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 — 20/100

Estado: FALLO

Faltan robots.txt y 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: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.

[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking donde un atacante puede cargar la web en un marco invisible.
[HIGH] Cookie HttpOnly: Las cookies googtrans y XSRF-TOKEN carecen de este flag, permitiendo que scripts de terceros accedan a ellas mediante JavaScript.
[HIGH] Cookie Secure: Las cookies googtrans, XSRF-TOKEN y laravel_session se envían sin el flag Secure, lo que permite su interceptación en conexiones no cifradas.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, aumentando el riesgo de ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a otros sitios, lo que podría filtrar URLs privadas del panel de usuario.
[MEDIUM] Permissions-Policy: El navegador no tiene restricciones sobre el uso de APIs como la cámara o el micrófono, aumentando la superficie de ataque.
[MEDIUM] Cookie SameSite: La cookie googtrans no restringe su envío en peticiones de origen cruzado, facilitando posibles ataques CSRF.
[MEDIUM] Puerto 8080 (HTTP-Alt) ABIERTO: La exposición de este puerto alternativo puede ser utilizada para evadir controles de seguridad o acceder a servicios internos.
[LOW] Server header expuesto: El servidor revela el uso de tecnología Cloudflare, lo cual facilita las etapas de reconocimiento para un atacante.