EscanearVulnerabilidades

Informe de Seguridad Web

URL	http://machine.fyva.ai/	Checks	9 pruebas
Dominio	machine.fyva.ai	Hallazgos	45 totales
Fecha	12 de mayo de 2026 a las 12:58	Problemas	7 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio machine.fyva.ai arroja una puntuación de 76/100, lo que equivale a una calificación de nota B. Durante la auditoría se ejecutaron 9 checks pasivos, resultando en 4 verificaciones satisfactorias, 3 advertencias y 1 fallo crítico en la configuración de cabeceras. Aunque el cifrado de datos es adecuado, se identificaron carencias importantes en las directivas de protección del navegador y una exposición innecesaria de puertos de red. En su estado actual, el sitio se considera moderadamente seguro pero presenta vulnerabilidades que podrían ser explotadas mediante ataques de inyección o suplantación de identidad. Es imperativo aplicar las correcciones técnicas detalladas para mitigar los riesgos detectados.

Resumen de Riesgos

0	3	2	2	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 85 dias
Cabeceras de Seguridad	45	FALLO	Solo 3/6 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	100	OK	1 cookies, todas con flags correctos
Contenido Mixto	50	AVISO	El sitio no usa HTTPS, no aplica chequeo de cont...
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 85 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  85 dias restantes (expira: 2026-08-05T13:28:24.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-07T12:28:36.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 45/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, 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; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://machine.fyva.ai/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS 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 — 100/100

Estado: OK

1 cookies, todas con flags correctos

- 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

- INFO **Cookie: __cf_bm — SameSite**
  SameSite=none

Contenido Mixto — 50/100

Estado: AVISO

El sitio no usa HTTPS, no aplica chequeo de contenido mixto

- ALTO **Protocolo**
  El sitio no usa HTTPS

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (160 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 5 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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 ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso en el navegador del usuario.
[HIGH] X-Frame-Options: Al no estar implementada, el sitio es vulnerable a ataques de clickjacking, permitiendo que atacantes carguen la web en marcos invisibles para robar clics.
[HIGH] Protocolo Inseguro: Se ha detectado que el sitio no utiliza HTTPS de forma consistente en todas sus comprobaciones, lo que pone en riesgo la integridad de la comunicación.
[MEDIUM] Permissions-Policy: La falta de esta directiva no restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono, aumentando el riesgo de privacidad.

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de un servidor web alternativo o proxy abierto incrementa la superficie de ataque y la posibilidad de accesos no autorizados.
[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando información técnica valiosa que facilita el perfilado del sitio por parte de atacantes.
[LOW] sitemap.xml ausente: La falta de un mapa del sitio dificulta la auditoría de rutas públicas y la indexación estructurada, pudiendo ocultar páginas no deseadas.