EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.akkeron.com	Checks	9 pruebas
Dominio	www.akkeron.com	Hallazgos	44 totales
Fecha	17 de septiembre de 2026 a las 08:51	Problemas	12 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al portal presenta una puntuación de 68/100 y una calificación de grado C. Los resultados de los checks pasivos indican que se ejecutaron 9 pruebas, obteniendo 5 resultados satisfactorios, 2 advertencias y 1 fallo crítico. Se ha detectado una implementación correcta del cifrado SSL, pero existen carencias graves en las cabeceras de seguridad y la presencia de servicios de red innecesarios. La falta de políticas de seguridad modernas y la exposición de versiones del sistema incrementan el riesgo operativo de la plataforma. Se concluye que el sitio es vulnerable y requiere atención técnica inmediata para mitigar posibles ataques de inyección y acceso no autorizado.

Resumen de Riesgos

0	5	3	4	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 84 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Seguridad de Cookies	100	OK	No se encontraron cookies
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): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 84 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  84 dias restantes (expira: 2026-12-10T11:32:23.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-11T11:32:24.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.33 — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://akkeron.com/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 7.1
- INFO **Tecnologias detectadas**
  Next.js, Astro, PHP/8.3.33

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (392 bytes)
- INFO **Reglas robots.txt**
  7 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://akkeron.com/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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] Puerto 21 (FTP) Abierto: El servicio de transferencia de archivos está expuesto, lo que permite el envío de datos sin cifrar y posibles ataques de fuerza bruta.
[HIGH] Ausencia de HSTS (Strict-Transport-Security): El sitio no obliga al navegador a usar conexiones HTTPS, permitiendo ataques de degradación de SSL.
[HIGH] Content-Security-Policy (CSP) Faltante: La falta de esta política facilita la ejecución de scripts maliciosos (XSS) y ataques de inyección de contenido.
[HIGH] X-Frame-Options Faltante: El sitio no está protegido contra ataques de clickjacking, permitiendo que la web sea cargada en marcos externos maliciosos.
[MEDIUM] X-Content-Type-Options Faltante: Al no estar configurada, el navegador podría intentar interpretar el contenido de forma distinta al tipo MIME declarado, arriesgando la ejecución de código.
[MEDIUM] Referrer-Policy y Permissions-Policy Faltantes: No se controla la información de procedencia enviada a terceros ni se restringen las APIs sensibles del navegador.
[LOW] Exposición de tecnología en cabeceras: Se revela el uso de servidor Apache y la versión PHP/8.3.33, facilitando el reconocimiento a posibles atacantes.

[LOW] Divulgación de versión del CMS: El metadato meta generator expone el uso de WordPress 7.1, permitiendo identificar vulnerabilidades específicas de la versión.
[LOW] Ruta administrativa en robots.txt: Se hace referencia a rutas tipo "admin", lo que orienta a atacantes sobre la ubicación de directorios sensibles.