EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.fahorro.com/?gad_source=1&gad_campaignid=22963550623&gclid=CjwKCAjwhaSjBhB-EiwAkZqxi_J_cvmFBF2T3YzfYGUaxjqm-yeKQC4LRGkenIO9mKFmkE_jsiapChoC4EkQAvD_BwE	Escaneos	1
Dominio	www.fahorro.com	Hallazgos	48 totales
Fecha	2 de julio de 2026 a las 14:38	Problemas	19 detectados

D

47/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web ha arrojado una puntuación de 47/100, lo que se traduce en una calificación de nota D. Se llevaron a cabo un total de 9 comprobaciones pasivas, de las cuales 4 resultaron exitosas, se generó 1 advertencia y se identificaron 4 fallos críticos de configuración. La infraestructura presenta debilidades significativas en la protección de datos de sesión y una exposición peligrosa de servicios internos. Tras evaluar estos resultados, se concluye que el sitio es actualmente vulnerable y requiere medidas correctivas urgentes para mitigar riesgos de intrusión.

Resumen de Riesgos

3	9	6	1	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 82 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	17	FALLO	visid_incap_2896117: falta Secure; visid_incap_2...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	20	FALLO	5 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 82 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  82 dias restantes (expira: 2026-09-22T03:38:08.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-24T03:38:08.000Z
- 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

- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 403 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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

- 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 — 17/100

Estado: FALLO

visid_incap_2896117: falta Secure; visid_incap_2896117: falta SameSite; incap_ses_611_2896117: falta HttpOnly; incap_ses_611_2896117: falta Secure; incap_ses_611_2896117: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)

- INFO **Cookie: visid_incap_2896117 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: visid_incap_2896117 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: visid_incap_2896117 — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: incap_ses_611_2896117 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: incap_ses_611_2896117 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: incap_ses_611_2896117 — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 (368 bytes)
- INFO **Reglas robots.txt**
  16 Disallow, 0 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

5 puertos riesgosos abiertos

- 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- CRITICO **Puerto 3389 (RDP)**
  ABIERTO — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- CRITICO **Puerto 6379 (Redis)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL): Servicio de base de datos expuesto directamente a internet, lo que permite intentos de acceso remoto y ataques de fuerza bruta.
[CRITICAL] Puerto 3389 (RDP): Protocolo de escritorio remoto visible, facilitando posibles ataques para tomar el control del servidor Windows.
[CRITICAL] Puerto 6379 (Redis): Sistema de caché accesible sin autenticación, lo que podría exponer datos temporales sensibles de los usuarios.
[HIGH] Puerto 21 (FTP): Uso de un protocolo de transferencia de archivos sin cifrar que permite la interceptación de credenciales en la red.
[HIGH] Falta de Content-Security-Policy: Ausencia de una política de seguridad de contenido, aumentando el riesgo de ataques XSS e inyección de scripts.
[HIGH] Falta de X-Frame-Options: El sitio no previene ser cargado dentro de marcos externos, lo que lo hace vulnerable a ataques de clickjacking.
[HIGH] Falta de Strict-Transport-Security: No se obliga al navegador a usar siempre conexiones cifradas, facilitando ataques de degradación de SSL.
[HIGH] Fallo en Redirección HTTPS: El servidor responde con error 403 en lugar de redirigir el tráfico inseguro de forma automática, dejando conexiones desprotegidas.
[HIGH] Cookie incap_ses_611_2896117 sin HttpOnly: La ausencia de este flag permite que scripts maliciosos accedan a la cookie de sesión a través del navegador.
[HIGH] Cookies sin flag Secure: Tanto visid_incap como incap_ses pueden ser enviadas a través de conexiones no cifradas, exponiéndolas a robos de sesión.
[MEDIUM] Cookies sin flag SameSite: Las cookies de sesión carecen de esta protección, dejando a los usuarios vulnerables a ataques de falsificación de solicitud en sitios cruzados (CSRF).
[MEDIUM] Falta de X-Content-Type-Options: Permite que el navegador ignore el tipo de contenido declarado, facilitando la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Falta de Referrer-Policy: No se controla cuánta información de navegación se comparte con sitios externos al hacer clic en enlaces.
[MEDIUM] Falta de Permissions-Policy: El sitio no restringe el acceso a funciones sensibles del dispositivo como cámara o geolocalización.
[MEDIUM] Puerto 8080 (HTTP-Alt): Servidor web alternativo activo que puede estar exponiendo interfaces de administración o servicios en desarrollo.
[LOW] Falta de sitemap.xml: El archivo de mapa del sitio no es accesible, lo que dificulta las auditorías de estructura y la indexación correcta.