EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://serva3.grupoarpada.com	Checks	9 pruebas
Dominio	serva3.grupoarpada.com	Hallazgos	38 totales
Fecha	17 de junio de 2026 a las 09:14	Problemas	8 detectados

C

66/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arroja una puntuación de 66/100, lo que corresponde a una calificación de grado C. Durante el proceso se ejecutaron 9 checks pasivos, resultando en 4 verificaciones correctas, 1 advertencia y 1 fallo crítico en la configuración de cabeceras. Aunque el cifrado de datos es sólido, la ausencia total de cabeceras de seguridad y problemas en la redirección HTTPS elevan el riesgo técnico. Se concluye que el sitio es actualmente vulnerable a ataques de inyección y suplantación de identidad debido a una configuración de servidor incompleta. No se detectó un sistema de gestión de contenidos (CMS) conocido, lo que reduce la superficie de ataque frente a exploits comunes de plataformas comerciales.

Resumen de Riesgos

0	3	4	1	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 52 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	0	ERROR	No se pudo verificar contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 52 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  52 dias restantes (expira: 2026-08-08T00:38:02.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-10T00:38:03.000Z
- 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: ERROR

No se pudo verificar la redireccion HTTPS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://serva3.grupoarpada.com/

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

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (28 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)

- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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

[ALTA] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[ALTA] X-Frame-Options: Al no estar definida, el sitio es susceptible a ataques de Clickjacking, permitiendo que atacantes carguen la web en marcos externos.
[ALTA] Strict-Transport-Security: La falta de HSTS impide forzar conexiones seguras, dejando a los usuarios vulnerables a ataques de degradación de SSL.
[MEDIA] X-Content-Type-Options: El servidor no previene el sniffing de tipos MIME, lo que podría facilitar la ejecución de archivos con contenido malicioso disfrazado.
[MEDIA] Referrer-Policy: No se controla la información de procedencia enviada en las peticiones, lo que puede exponer rutas internas sensibles a terceros.
[MEDIA] Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como la cámara o el micrófono, incrementando el riesgo de privacidad.
[MEDIA] Bloqueo total en robots.txt: El archivo bloquea el rastreo de todo el sitio mediante la directiva Disallow, lo cual suele ser una configuración de desarrollo olvidada en producción.
[BAJA] sitemap.xml: No se encontró el mapa del sitio, lo que dificulta la auditoría de rutas y la indexación correcta de los recursos web.