EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://triarchmarket.com	Checks	9 pruebas
Dominio	triarchmarket.com	Hallazgos	47 totales
Fecha	24 de agosto de 2026 a las 22:55	Problemas	15 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre triarchmarket.com ha resultado en una puntuación de 72/100, lo que otorga al sitio una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo 6 resultados satisfactorios, 2 advertencias por configuraciones mejorables y 1 fallo crítico relacionado con la seguridad del servidor. Aunque el cifrado base es correcto, la ausencia total de cabeceras de protección expone la plataforma a ataques conocidos de inyección y suplantación. Se concluye que el sitio es vulnerable en su configuración de endurecimiento (hardening), requiriendo medidas correctivas inmediatas para alcanzar un nivel de seguridad óptimo.

Resumen de Riesgos

0	4	9	2	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 77 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
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): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 77 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  77 dias restantes (expira: 2026-11-09T12:17:36.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-11T12:17:37.000Z
- 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: Caddy — 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
- 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 308 redirige a https://triarchmarket.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

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

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente

- INFO **Version CMS**
  No se detecta ninguna version expuesta

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 (1041 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 2 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://triarchmarket.com/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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] Falta de Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de Cross-Site Scripting (XSS).
[HIGH] Falta de X-Frame-Options: El sitio es susceptible a ataques de clickjacking al permitir que el contenido sea embebido en marcos externos no autorizados.
[HIGH] Falta de Strict-Transport-Security (HSTS): El servidor no obliga al navegador a usar conexiones seguras, permitiendo ataques de degradación de protocolo (SSL Stripping).
[MEDIUM] Puerto 22 (SSH) abierto: El servicio de administración remota está expuesto a Internet, facilitando intentos de acceso por fuerza bruta.
[MEDIUM] Falta de X-Content-Type-Options: El navegador podría intentar interpretar archivos como un tipo MIME diferente al declarado, facilitando la ejecución de malware.
[MEDIUM] Paneles de login expuestos (/wp-login.php, /administrator/, /user/login): La accesibilidad pública de estas rutas facilita el descubrimiento de vectores de ataque administrativo.
[MEDIUM] Archivos informativos accesibles (/readme.html, /README.txt): Estos archivos pueden revelar metadatos técnicos o versiones de software que ayudan a un atacante en la fase de reconocimiento.
[MEDIUM] Falta de Referrer-Policy: No existe control sobre la información de navegación que se envía a sitios externos mediante los enlaces.
[MEDIUM] Falta de Permissions-Policy: No se restringe el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[LOW] Cabecera de servidor expuesta: El valor "Server: Caddy" revela la tecnología exacta utilizada, permitiendo a atacantes buscar vulnerabilidades específicas para ese software.
[LOW] Ruta sensible en robots.txt: La mención directa a directorios como "admin" ofrece pistas sobre la estructura interna del servidor a actores malintencionados.