EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://starsteamgt.com	Checks	9 pruebas
Dominio	starsteamgt.com	Hallazgos	46 totales
Fecha	19 de mayo de 2026 a las 22:07	Problemas	14 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio starsteamgt.com ha resultado en una puntuación de 62/100, lo que otorga una nota de C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 3 generaron advertencias y 2 fallaron debido a deficiencias críticas en la configuración. Aunque el cifrado de datos es funcional, la exposición de versiones obsoletas del CMS y la ausencia de cabeceras de protección incrementan el riesgo de compromiso. Se concluye que el sitio es actualmente vulnerable a ataques dirigidos y automatizados.

Resumen de Riesgos

0	5	6	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 89 dias
Cabeceras de Seguridad	10	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 3.3.6 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 89 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  89 dias restantes (expira: 2026-08-17T01:39:12.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-19T00:40:26.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 10/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-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
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- 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://starsteamgt.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: Site Kit by Google 1.178.0

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 3.3.6 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 3.3.6 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.acmethemes.com/

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (318 bytes)
- INFO **Reglas robots.txt**
  6 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://starsteamgt.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): 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] WordPress versión expuesta: Se detectó la versión 3.3.6 — El uso de versiones obsoletas permite a atacantes explotar múltiples vulnerabilidades conocidas (CVEs).
[HIGH] Content-Security-Policy: Falta — La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: Falta — Esta omisión hace que el sitio sea susceptible a ataques de clickjacking, donde un atacante puede engañar al usuario.
[HIGH] Strict-Transport-Security: Falta — Sin HSTS, el navegador no fuerza conexiones HTTPS, permitiendo posibles degradaciones de seguridad en la comunicación.
[MEDIUM] X-Content-Type-Options: Falta — Al no estar configurada, el navegador podría realizar sniffing de tipos MIME, ejecutando archivos no seguros.
[MEDIUM] Permissions-Policy: Falta — No se restringe el acceso de las APIs del navegador, dejando expuestas funciones como la cámara o el micrófono.
[MEDIUM] Archivo /readme.html: Accesible públicamente — Este archivo revela información técnica sobre el CMS que facilita la fase de reconocimiento de un atacante.
[MEDIUM] Ruta /wp-login.php: Panel de login accesible — La exposición directa del panel administrativo permite intentos de acceso no autorizados por fuerza bruta.
[MEDIUM] Contenido Mixto: Recurso HTTP detectado — Se carga una hoja de estilos externa desde acmethemes.com sin cifrado, comprometiendo la integridad de la página.
[MEDIUM] Puerto 8080 (HTTP-Alt): Abierto — La exposición de puertos alternativos aumenta la superficie de ataque y puede alojar servicios no supervisados.
[LOW] Server header expuesto: Revela Cloudflare — Proporciona información sobre la infraestructura de red utilizada, ayudando a perfilar el objetivo.
[LOW] Meta generator expuesto: Site Kit by Google 1.178.0 — Entrega detalles adicionales sobre los complementos y la configuración interna del sitio.
[LOW] Ruta sensible en robots.txt: Referencia a admin — Indica a los motores de búsqueda y atacantes la ubicación de directorios que deberían permanecer privados.