

EscanearVulnerabilidades

Informe de Seguridad Web

URL http://playgta5.com/
Dominio playgta5.com
Fecha 6 de octubre de 2026 a las 13:53

Checks 9 pruebas
Hallazgos 16 totales
Problemas 4 detectados

C

64/100

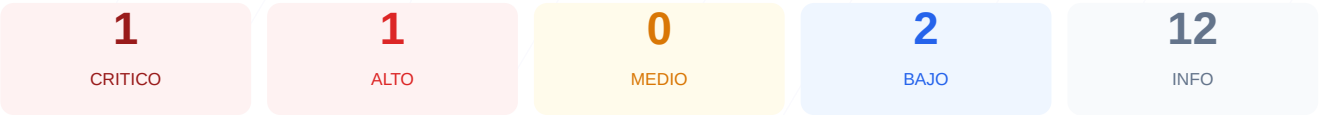
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación exacta de 64/100, lo que representa una nota de grado C. Durante la evaluación se ejecutaron 9 checks pasivos que resultaron en 1 prueba superada, 1 advertencia y 1 fallo crítico detectado en la estructura base. Se ha identificado una ausencia total de protocolos de cifrado, lo que impide validar la identidad del servidor y la privacidad de los datos. Debido a estas carencias técnicas fundamentales, se concluye que el sitio es vulnerable y no cumple con los estándares mínimos de seguridad actuales.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	50	AVISO	El sitio no usa HTTPS, no aplica chequeo de cont...
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO Conexion SSL
No se pudo establecer conexion SSL/TLS

Contenido Mixto — 50/100

Estado: AVISO

El sitio no usa HTTPS, no aplica chequeo de contenido mixto

- ALTO Protocolo
El sitio no usa HTTPS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO robots.txt
Error al acceder

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

	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 — Envío de correo
	INFO	Puerto 80 (HTTP)	Cerrado — Servidor web
	INFO	Puerto 443 (HTTPS)	Cerrado — 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 autentificacion 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

[CRITICAL] Conexion SSL: No se pudo establecer una conexion SSL/TLS, lo que significa que el sitio no cifra la informacion transmitida.
[HIGH] Protocolo HTTP: El sitio no utiliza HTTPS, permitiendo que cualquier dato intercambiado sea capturado por atacantes en la red.
[LOW] Archivo robots.txt: No se pudo acceder o no existe el archivo de directivas para buscadores, afectando el control de indexacion.
[LOW] Archivo sitemap.xml: Ausencia de mapa del sitio, lo que dificulta la auditoria de rutas y la navegacion de rastreadores legatarios.
[CRITICAL] Cabeceras de Seguridad: No se detectaron cabeceras de proteccion, dejando a los usuarios expuestos a ataques de inyeccion y suplantacion.