EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://siged.sie.gob.bo/	Checks	9 pruebas
Dominio	siged.sie.gob.bo	Hallazgos	47 totales
Fecha	30 de junio de 2026 a las 02:05	Problemas	7 detectados

B

81/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio siged.sie.gob.bo ha determinado una puntuación de 81/100, lo que equivale a una nota B. Se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, se generó 1 advertencia y se identificaron 2 fallos en la configuración. El sitio presenta una infraestructura base sólida en cuanto a cifrado, pero muestra debilidades críticas en la protección de sesiones y en la prevención de ataques de inyección. Debido a la falta de políticas de seguridad modernas y configuraciones de cookies inadecuadas, el sitio se clasifica como vulnerable ante ataques dirigidos contra el usuario final.

Resumen de Riesgos

0	2	2	3	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 35 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	33	FALLO	PHPSESSID: falta Secure; PHPSESSID: falta SameSi...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 35 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  35 dias restantes (expira: 2026-08-03T16:23:38.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-05T16:23:39.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff, nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer, strict-origin-when-cross-origin
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://siged.sie.gob.bo/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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

- 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 — 33/100

Estado: FALLO

PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: PHPSESSID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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 — Envio 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 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] Content-Security-Policy: Falta esta cabecera esencial, lo que permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] Cookie PHPSESSID sin flag Secure: La cookie de sesión se transmite sin protección, permitiendo que sea interceptada en conexiones que no sean estrictamente cifradas.
[MEDIUM] Cookie PHPSESSID sin flag SameSite: La ausencia de este atributo hace que el sitio sea susceptible a ataques de Cross-Site Request Forgery (CSRF).
[MEDIUM] Permissions-Policy: No se han definido restricciones para las APIs del navegador, permitiendo potencialmente el acceso a la cámara o micrófono desde el contexto web.
[LOW] Server header expuesto: El servidor revela el uso de nginx, proporcionando información técnica valiosa a posibles atacantes para buscar exploits específicos.
[LOW] robots.txt no encontrado: El archivo de instrucciones para rastreadores no existe, lo que impide gestionar adecuadamente la indexación del sitio.
[LOW] sitemap.xml no encontrado: La falta de un mapa del sitio dificulta la auditoría de rutas y la navegación estructurada por motores de búsqueda.