EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://geobuses.com/	Checks	9 pruebas
Dominio	geobuses.com	Hallazgos	46 totales
Fecha	19 de junio de 2026 a las 21:23	Problemas	12 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio geobuses.com arroja una puntuación de 61/100, obteniendo una calificación de nota C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, uno presentó advertencias y dos fallaron de forma crítica. El sitio web muestra una implementación deficiente de medidas de protección fundamentales en el servidor y una gestión de tráfico cifrado incompleta. En su estado actual, se concluye que el sitio es vulnerable ante ataques comunes debido a la ausencia de políticas de seguridad esenciales.

Resumen de Riesgos

0	5	4	3	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 38 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 38 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  38 dias restantes (expira: 2026-07-28T09:11:53.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-29T08:14:22.000Z
- 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: cloudflare — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PleskLin — Revela framework/lenguaje
- 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: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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
- BAJO **Meta generator**
  Expone: Astro v6.2.2
- INFO **Tecnologias detectadas**
  Astro, PleskLin

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 — 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 (336 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 6 Allow
- INFO **Sitemap en robots.txt**
  https://geobuses.com/sitemap-index.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] Falta de redirección HTTPS: El servidor no redirige automáticamente el tráfico HTTP a HTTPS, permitiendo conexiones inseguras donde los datos viajan en texto plano.
[HIGH] Ausencia de HSTS (Strict-Transport-Security): El sitio no instruye a los navegadores para usar exclusivamente conexiones seguras, facilitando ataques de degradación de SSL.
[HIGH] Falta de Content-Security-Policy (CSP): No existe una política que restrinja el origen de los recursos, lo que hace al sitio altamente vulnerable a ataques de Cross-Site Scripting (XSS).
[HIGH] Falta de X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea cargado en iframes externos, exponiéndolo a ataques de clickjacking.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de servicios en puertos alternativos no estándar aumenta la superficie de ataque y puede revelar servicios internos vulnerables.
[MEDIUM] Falta de cabeceras de seguridad adicionales: La carencia de X-Content-Type-Options, Referrer-Policy y Permissions-Policy impide mitigar riesgos de MIME-sniffing y filtración de datos de navegación.
[LOW] Exposición de tecnología en cabeceras: Se revelan detalles específicos del servidor (Cloudflare) y del panel de control (PleskLin), lo que ayuda a un atacante en la fase de reconocimiento.
[LOW] Versión de tecnología expuesta: La etiqueta meta generator expone el uso de Astro v6.2.2, permitiendo la búsqueda de exploits específicos para dicha versión.