EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.slgu.com.ar	Checks	9 pruebas
Dominio	www.slgu.com.ar	Hallazgos	45 totales
Fecha	21 de agosto de 2026 a las 22:13	Problemas	10 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis técnico de seguridad realizado arroja una puntuación de 65/100, lo que sitúa al sitio web en una nota de grado C. Durante la evaluación se ejecutaron un total de 9 comprobaciones pasivas, resultando 7 satisfactorias y 2 con fallos críticos relacionados con la configuración del servidor. A pesar de contar con un cifrado SSL válido, la carencia absoluta de cabeceras de protección y errores en la gestión del protocolo HTTPS elevan el perfil de riesgo. Se concluye que el sitio es vulnerable ante ataques de intermediario y técnicas de inyección de contenido. La infraestructura requiere ajustes inmediatos para alinearse con los estándares mínimos de seguridad web vigentes.

Resumen de Riesgos

0	5	3	2	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 46 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	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 46 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  46 dias restantes (expira: 2026-10-06T14:36:35.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-08T14:36:36.000Z
- 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: Apache/2.4.46 (Unix) OpenSSL/1.0.1e-fips mod_fastcgi/mod_fastcgi-SNAP-0910052141 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/5.6.40 — 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 503 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 503

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
- INFO **Tecnologias detectadas**
  PHP/5.6.40

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 (350 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://slgu.com.ar/?sitemapindex.xml
- 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] Redirección HTTPS fallida: El servidor no redirige automáticamente las conexiones inseguras a HTTPS, devolviendo un error de estado 503.

[HIGH] Content-Security-Policy (CSP) ausente: La falta de esta política permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] X-Frame-Options ausente: El sitio es susceptible a ataques de clickjacking, permitiendo que atacantes carguen la web en marcos invisibles para engañar usuarios.
[HIGH] Strict-Transport-Security (HSTS) ausente: No se instruye al navegador para que utilice exclusivamente conexiones cifradas, facilitando ataques de degradación de protocolo.
[MEDIUM] X-Content-Type-Options ausente: La ausencia de la directiva nosniff permite que el navegador interprete erróneamente tipos de archivos, facilitando la ejecución de malware.
[MEDIUM] Referrer-Policy ausente: El servidor no controla qué información de procedencia se envía a terceros, comprometiendo la privacidad de la navegación.
[MEDIUM] Permissions-Policy ausente: No existen restricciones sobre el uso de funciones sensibles del navegador como geolocalización o periféricos.
[LOW] Exposición de cabecera Server: La respuesta del servidor revela el uso de Apache/2.4.46 y OpenSSL/1.0.1e, facilitando la identificación de exploits específicos.
[LOW] Exposición de cabecera X-Powered-By: Se divulga el uso de PHP/5.6.40, una versión antigua que permite a un atacante perfilar mejor sus vectores de ataque.