

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://evaluaciones.luisgonzaganeiraayala.com/dojo/student/67	Checks	9 pruebas
Dominio	evaluaciones.luisgonzaganeiraayala.com	Hallazgos	46 totales
Fecha	10 de septiembre de 2026 a las 03:55	Problemas	9 detectados

C

74/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el sitio web ha arrojado una puntuación de 74/100, lo que se traduce en una calificación de grado C. Durante el proceso se ejecutaron 9 comprobaciones pasivas, de las cuales 6 resultaron satisfactorias, 2 presentaron advertencias y 1 fue calificada como fallo crítico. Los resultados indican que, si bien la base del cifrado es sólida, existe una carencia absoluta de protecciones contra ataques de inyección y suplantación a nivel de servidor. Por tanto, se concluye que el sitio es parcialmente vulnerable y requiere ajustes inmediatos para alcanzar un nivel de seguridad robusto.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 75 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	1 cookies, todas con flags correctos
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 75 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
75 dias restantes (expira: 2026-11-24T13:39:46.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-26T13:39:47.000Z
- 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: nginx — 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
- MEDIO

Referrer-Policy
Falta — Controla la informacion de referer enviada
- 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://evaluaciones.luisgonzaganeiraayala.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

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 — 100/100

Estado: OK

1 cookies, todas con flags correctos

- INFO

Cookies detectadas
1 cookie(s) encontrada(s)
- INFO

Cookie: evaluaciones_session — HttpOnly
HttpOnly activo — No accesible via JavaScript
- INFO

Cookie: evaluaciones_session — Secure
Flag Secure activo — Solo se envia por HTTPS
- INFO

Cookie: evaluaciones_session — SameSite
SameSite=lax

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO

robots.txt
Presente (66 bytes)
- INFO

Reglas robots.txt
0 Disallow, 0 Allow
- 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: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.

[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking, permitiendo que terceros carguen la página en marcos invisibles.

[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador obligue siempre el uso de conexiones cifradas, facilitando ataques de degradación de protocolo.

[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite el MIME-type sniffing, lo que puede llevar al navegador a interpretar archivos de forma insegura.

[MEDIUM] Referrer-Policy: No se define qué información de procedencia se envía a otros sitios, lo que puede exponer datos privados de la navegación.

[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la ubicación geográfica.

[LOW] Server header expuesto: La cabecera revela el uso de la tecnología nginx, proporcionando información valiosa a posibles atacantes para buscar exploits específicos.

[LOW] sitemap.xml: El archivo de mapa del sitio no fue encontrado, lo que dificulta la indexación correcta y el análisis de la estructura por herramientas legítimas.