# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://siam5.io/bas_Login/ | Checks | 9 pruebas |
| Dominio | siam5.io | Hallazgos | 50 totales |
| Fecha | 4 de septiembre de 2026 a las 16:17 | Problemas | 6 detectados |

**B**

85/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio siam5.io ha arrojado una puntuación de 85/100, lo que corresponde a una nota B. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo como resultado 5 verificaciones satisfactorias, 3 advertencias y 1 fallo crítico en la configuración de archivos de indexación. Aunque el sitio demuestra una implementación sólida de cifrado TLS y redirecciones seguras, la ausencia de políticas de seguridad modernas y la exposición de puertos administrativos elevan el nivel de riesgo. Se concluye que el sitio es generalmente estable, pero permanece vulnerable a ataques de inyección y de denegación de servicio si no se corrigen las debilidades detectadas.

## Resumen de Riesgos

| 0 | 1 | 2 | 3 | 44 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 88 dias |
| Cabeceras de Seguridad | 75 | AVISO | 5/6 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 | 83 | AVISO | sc_actual_lang_Siglope: falta SameSite |
| Contenido Mixto | 100 | OK | No se detecto contenido mixto |
| Robots.txt y Sitemap | 20 | FALLO | Faltan robots.txt y sitemap.xml |
| Puertos Abiertos | 60 | AVISO | 1 puerto(s) potencialmente riesgoso(s): 22 (SSH) |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 88 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  88 dias restantes (expira: 2026-12-01T16:05:40.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-02T16:05:41.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

## Cabeceras de Seguridad — 75/100

Estado: AVISO

5/6 presentes. Faltan: Content-Security-Policy

- BAJO **Server header expuesto**
  Server: Apache/2.4.66 (Ubuntu) — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: camera=(), microphone=(), geolocation=()

## Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://siam5.io/
- 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 — 83/100

Estado: AVISO

sc_actual_lang_Siglope: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: PHPSESSID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: PHPSESSID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: PHPSESSID — SameSite**
  SameSite=lax
- INFO **Cookie: sc_actual_lang_Siglope — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: sc_actual_lang_Siglope — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: sc_actual_lang_Siglope — 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 — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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
- 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 facilita la ejecución de ataques Cross-Site Scripting (XSS) y la inyección de contenido malicioso por parte de terceros.
[MEDIUM] Cookie sc_actual_lang_Siglope: El atributo SameSite no está definido, lo que expone a los usuarios a riesgos de Cross-Site Request Forgery (CSRF).
[MEDIUM] Puerto 22 (SSH) abierto: La detección de un puerto de acceso remoto abierto aumenta la superficie de ataque, permitiendo intentos de intrusión por fuerza bruta si no está restringido por IP.
[LOW] Server header expuesto: El servidor revela la versión exacta Apache/2.4.66 (Ubuntu), facilitando a un atacante la búsqueda de exploits específicos para esa tecnología.
[LOW] robots.txt no encontrado: La falta de este archivo impide controlar qué partes del sitio deben o no ser rastreadas por motores de búsqueda.
[LOW] sitemap.xml no encontrado: La ausencia de un mapa del sitio dificulta la correcta indexación y el análisis de la estructura del directorio por herramientas de auditoría.