EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://appemvarias.com/siglope/bas_Login/	Checks	9 pruebas
Dominio	appemvarias.com	Hallazgos	48 totales
Fecha	21 de abril de 2026 a las 19:39	Problemas	12 detectados

C

71/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad web realizada al portal arroja una puntuacion de 71/100, lo que corresponde a una nota C. El analisis se baso en 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 genero una advertencia y 3 fallaron criticamente. Aunque el cifrado de datos basico esta presente, existen deficiencias importantes en la configuracion de cabeceras de seguridad y en la proteccion de sesiones. Debido a la ausencia de mecanismos de endurecimiento (hardening) y politicas de cookies debiles, el sitio se clasifica actualmente como vulnerable ante ataques de interceptacion y suplantacion de identidad.

Resumen de Riesgos

0	6	3	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 53 dias
Cabeceras de Seguridad	40	FALLO	Solo 3/6 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	17	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 53 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  53 dias restantes (expira: 2026-06-13T15:35:57.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-15T15:35:58.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 40/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, 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: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff, nosniff
- INFO **Referrer-Policy**
  Presente: same-origin
- 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://appemvarias.com/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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 — 17/100

Estado: FALLO

PHPSESSID: falta Secure; PHPSESSID: falta SameSite; sc_actual_lang_Siglope: falta HttpOnly; sc_actual_lang_Siglope: falta Secure; sc_actual_lang_Siglope: falta SameSite

- INFO **Cookies detectadas**
  2 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
- ALTO **Cookie: sc_actual_lang_Siglope — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: sc_actual_lang_Siglope — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- 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 — 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 ejecucion de scripts no autorizados, facilitando ataques de Cross-Site Scripting (XSS) e inyeccion de contenido malicioso.
[HIGH] Strict-Transport-Security: No se detecto la cabecera HSTS, lo que permite que un atacante intente degradar la conexion a HTTP para interceptar datos sensibles.
[HIGH] Cookie PHPSESSID (Secure): La cookie de sesion carece del flag Secure, permitiendo que sea transmitida a traves de conexiones no cifradas y aumentando el riesgo de robo de sesion.
[HIGH] Cookie sc_actual_lang_Siglope (HttpOnly/Secure): Esta cookie no tiene proteccion contra acceso por scripts ni obligatoriedad de transmision cifrada, siendo vulnerable a filtraciones mediante ataques XSS.
[MEDIUM] Permissions-Policy: La falta de esta configuracion impide restringir el acceso del navegador a funciones sensibles como la camara o el microfono, exponiendo la privacidad del usuario.
[MEDIUM] Cookie SameSite: Ambas cookies analizadas carecen del atributo SameSite, lo que deja el portal expuesto a ataques de falsificacion de peticiones en sitios cruzados (CSRF).
[LOW] Server header expuesto: El servidor revela el uso de nginx, lo cual proporciona informacion valiosa a posibles atacantes para buscar exploits especificos de esa tecnologia.
[LOW] Ausencia de archivos de control: No se encontraron los archivos robots.txt ni sitemap.xml, lo que afecta el control sobre la indexacion y el rastreo del sitio.