EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://votacion.panamericana.pe/la-granja/registrar	Checks	9 pruebas
Dominio	votacion.panamericana.pe	Hallazgos	50 totales
Fecha	16 de abril de 2026 a las 12:19	Problemas	11 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis técnico de ciberseguridad ha determinado una puntuación de 70/100, otorgando una calificación de C al activo evaluado. Durante el proceso se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias y 1 fue clasificado como fallo crítico. Se han detectado debilidades importantes en la configuración de las cabeceras de seguridad y en la gestión de atributos de las cookies de sesión. Debido a la ausencia de mecanismos de defensa fundamentales como CSP y HSTS, se concluye que el sitio es actualmente vulnerable ante ataques de intermediarios e inyecciones de código.

Resumen de Riesgos

0	6	3	2	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 250 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	CMS detectado: WordPress
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	67	AVISO	XSRF-TOKEN: falta HttpOnly; encuestasptv_session...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 250 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  250 dias restantes (expira: 2026-12-22T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-12-23T00:00:00.000Z
- 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 **X-Powered-By expuesto**
  X-Powered-By: PHP/8.5.4 — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://votacion.panamericana.pe:443/
- 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

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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/8.5.4

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 — 67/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly; encuestasptv_session: falta Secure

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: encuestasptv_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: encuestasptv_session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: encuestasptv_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 (24 bytes)
- INFO **Reglas robots.txt**
  1 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

2 puerto(s) abierto(s), todos esperados

- 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

- 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 ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: No está configurada, lo que expone a los usuarios a riesgos de clickjacking mediante el secuestro de la interfaz.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones cifradas, permitiendo ataques de degradación de SSL.
[HIGH] Cookie XSRF-TOKEN: Carece del flag HttpOnly, permitiendo que la cookie sea accesible mediante scripts, elevando el riesgo de robo de sesión.
[HIGH] Cookie encuestasptv_session: No tiene el flag Secure, lo que implica que la información de sesión podría transmitirse a través de canales no cifrados.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador puede intentar adivinar el tipo de contenido, facilitando la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: La falta de control sobre esta política puede filtrar información sensible de la URL a dominios externos.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs del navegador, dejando expuestas funciones como cámara, micrófono o geolocalización.
[LOW] X-Powered-By: La cabecera expone el uso de PHP/8.5.4, facilitando a un atacante la búsqueda de vulnerabilidades específicas para esa versión.
[LOW] sitemap.xml: El archivo no fue localizado, lo que afecta la transparencia de la estructura del sitio y su auditoría.