EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sisrecaudacion.unasam.edu.pe	Checks	9 pruebas
Dominio	sisrecaudacion.unasam.edu.pe	Hallazgos	50 totales
Fecha	12 de julio de 2026 a las 08:45	Problemas	15 detectados

D

56/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar una evaluación técnica de ciberseguridad, el sitio web ha obtenido una puntuación de 56/100, lo que equivale a una calificación de D. Durante el análisis se ejecutaron 9 checks pasivos, de los cuales 3 resultaron satisfactorios, 4 generaron advertencias y 2 fueron marcados como fallos críticos. La infraestructura presenta debilidades significativas en la configuración de cabeceras de seguridad y, sobre todo, en la exposición de servicios críticos de bases de datos a la red pública. Por estos motivos, se concluye que el sitio es actualmente vulnerable y requiere intervenciones correctivas urgentes para mitigar riesgos de filtración de datos.

Resumen de Riesgos

2	7	4	2	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	70	AVISO	Certificado expira en 28 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	50	AVISO	XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Se...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 70/100

Estado: AVISO

Certificado expira en 28 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- MEDIO **Dias hasta expiracion**
  28 dias restantes (expira: 2026-08-09T01:42:39.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-11T01:42:40.000Z
- 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: openresty — 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://sisrecaudacion.unasam.edu.pe/
- 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
- INFO **Tecnologias detectadas**
  Next.js

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 — 50/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Secure; tesoreria_unasam_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)
- ALTO **Cookie: XSRF-TOKEN — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: tesoreria_unasam_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: tesoreria_unasam_session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: tesoreria_unasam_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 — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL): La base de datos MySQL se encuentra abierta y accesible desde internet, lo que permite intentos de acceso no autorizados y ataques directos contra la información.
[CRITICAL] Puerto 5432 (PostgreSQL): El servicio de base de datos PostgreSQL está expuesto públicamente, representando un riesgo extremo de exfiltración de datos institucionales.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: El sitio no cuenta con protección contra clickjacking, permitiendo que la interfaz sea embebida en marcos maliciosos para engañar a los usuarios.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones cifradas, dejando la comunicación vulnerable a ataques de degradación de protocolo.
[HIGH] Cookie XSRF-TOKEN (HttpOnly): Al carecer del flag HttpOnly, la cookie es accesible mediante scripts del lado del cliente, aumentando el riesgo de robo de sesión.
[HIGH] Cookie XSRF-TOKEN (Secure): La cookie no tiene el flag Secure, por lo que puede ser transmitida a través de conexiones HTTP no cifradas.
[HIGH] Cookie tesoreria_unasam_session (Secure): El identificador de sesión se envía sin protección de cifrado obligatorio, facilitando su intercepción en la red.
[MEDIUM] X-Content-Type-Options: El servidor no previene el MIME-type sniffing, lo que podría permitir al navegador ejecutar archivos con tipos MIME incorrectos.
[MEDIUM] Referrer-Policy: No existe una política definida para el control de la información de procedencia que se comparte con otros dominios.
[MEDIUM] Permissions-Policy: No se han restringido las APIs del navegador, dejando activos permisos para componentes como cámara o micrófono innecesariamente.
[MEDIUM] Puerto 22 (SSH): El puerto de administración remota está abierto, quedando expuesto a ataques de fuerza bruta si no está debidamente restringido por IP.
[LOW] Server header expuesto: La cabecera revela el uso de openresty, proporcionando información técnica valiosa a posibles atacantes para identificar vulnerabilidades específicas.
[LOW] sitemap.xml: La ausencia de este archivo dificulta la auditoría de rutas legítimas y la correcta indexación de los recursos del sitio.