EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cid.unasam.edu.pe	Checks	9 pruebas
Dominio	cid.unasam.edu.pe	Hallazgos	53 totales
Fecha	12 de julio de 2026 a las 08:41	Problemas	20 detectados

D

51/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría técnica realizada al sitio web arroja una puntuación de 51/100, lo que equivale a una nota D. Se ejecutaron 9 checks pasivos, de los cuales solo 2 resultaron satisfactorios, mientras que se identificaron 2 advertencias y 5 fallos críticos. El análisis revela deficiencias severas en la configuración de cabeceras de seguridad, protección de cookies y una exposición peligrosa de servicios de base de datos. Debido a la presencia de múltiples vectores de ataque abiertos y configuraciones incorrectas, se concluye que el sitio es actualmente vulnerable y presenta un riesgo significativo para la integridad de la infraestructura.

Resumen de Riesgos

2	6	9	3	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	70	AVISO	Certificado expira en 28 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	CMS detectado: Wix
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	17	FALLO	XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Se...
Contenido Mixto	20	FALLO	6 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y 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 — 40/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, 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
- INFO **X-Frame-Options**
  Presente: DENY
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer
- 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://cid.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

CMS detectado: Wix

- 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**
  Detectado via HTML body
- 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)
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 17/100

Estado: FALLO

XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Secure; XSRF-TOKEN: falta SameSite; laravel_session: falta Secure; laravel_session: falta SameSite

- 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
- MEDIO **Cookie: XSRF-TOKEN — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: laravel_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: laravel_session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: laravel_session — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 20/100

Estado: FALLO

6 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://fonts.googleapis.com/css?family=Lato:300,400,700,300i...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://fonts.googleapis.com/css?family=Raleway:400,300,700
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://cid.unasam.edu.pe/
- MEDIO **href (link/stylesheet)**
  ...y 3 mas del mismo tipo

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 500)
- BAJO **sitemap.xml**
  No encontrado (HTTP 500)
- 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): Base de datos MySQL expuesta directamente a internet, permitiendo intentos de intrusión y ataques de fuerza bruta externos.
[CRITICAL] Puerto 5432 (PostgreSQL): Servicio de base de datos PostgreSQL accesible públicamente, lo que facilita la explotación de vulnerabilidades en el motor de datos.
[HIGH] Content-Security-Policy (CSP): Ausencia de esta cabecera, lo que deja el sitio vulnerable a ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] Strict-Transport-Security (HSTS): No se fuerza el uso de HTTPS a nivel de navegador, permitiendo ataques de degradación de conexión (downgrade attacks).
[HIGH] Cookie XSRF-TOKEN: Carece de los flags HttpOnly y Secure, permitiendo que la cookie sea accesible mediante scripts y enviada por canales no cifrados.
[HIGH] Cookie laravel_session: Falta el flag Secure, lo que expone el identificador de sesión si el tráfico es interceptado en conexiones no cifradas.
[MEDIUM] Contenido Mixto: Presencia de 6 recursos cargados mediante HTTP en una página protegida por HTTPS, lo que compromete la seguridad global del cifrado.
[MEDIUM] Puerto 22 (SSH): El puerto de gestión remota está abierto, aumentando la superficie de ataque frente a intentos de acceso no autorizados al servidor.
[MEDIUM] Cookies SameSite: Las cookies de sesión no tienen configurado el atributo SameSite, haciéndolas susceptibles a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Panel de Login: La ruta /user/login es accesible de forma pública, facilitando el reconocimiento y ataques dirigidos contra cuentas administrativas.
[LOW] Certificado SSL: El certificado digital expira en 28 días, lo que requiere una gestión de renovación inmediata para evitar alertas de seguridad a los usuarios.
[LOW] Server header: La cabecera revela el uso de openresty, proporcionando información técnica específica que ayuda a los atacantes a buscar exploits conocidos.
[LOW] Archivos de indexación: No se encontraron robots.txt ni sitemap.xml (error 500), dificultando la auditoría de acceso y el control de rastreo.