EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://clinicaempresarial.unasam.edu.pe/login	Checks	9 pruebas
Dominio	clinicaempresarial.unasam.edu.pe	Hallazgos	48 totales
Fecha	12 de julio de 2026 a las 08:53	Problemas	12 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web clinicaempresarial.unasam.edu.pe ha resultado en una puntuación de 61/100, lo que otorga una nota de C. Durante el análisis se ejecutaron 9 checks pasivos, de los cuales 3 resultaron satisfactorios, 4 generaron advertencias y 2 fueron calificados como fallos críticos. Aunque el sitio cuenta con cifrado SSL, la exposición de servicios internos y la carencia total de cabeceras de seguridad incrementan significativamente la superficie de ataque. Debido a estos hallazgos, se concluye que el sitio es actualmente vulnerable ante ataques de interceptación de datos y explotación de servicios. No se ejecutó un pentest activo en esta sesión de escaneo.

Resumen de Riesgos

1	5	3	3	36
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	83	AVISO	XSRF-TOKEN: falta HttpOnly
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): 3306 (My...

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: nginx/1.24.0 (Ubuntu) — 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://clinicaempresarial.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

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

XSRF-TOKEN: falta HttpOnly

- 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: clinica_empresarial_fec_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: clinica_empresarial_fec_session — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: clinica_empresarial_fec_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 — 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): 3306 (MySQL)

- 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL): La base de datos se encuentra abierta y expuesta a internet, permitiendo intentos de conexión externa y ataques de fuerza bruta.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de ataques Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: No existe protección contra clickjacking, lo que permite que el sitio sea embebido en marcos externos para engañar a los usuarios.
[HIGH] Strict-Transport-Security: La falta de configuración HSTS impide que el navegador obligue siempre el uso de conexiones seguras, facilitando ataques de degradación de protocolo.
[HIGH] Cookie XSRF-TOKEN - HttpOnly: La cookie de seguridad carece del atributo HttpOnly, lo que la hace accesible mediante scripts y vulnerable al robo de sesiones.
[MEDIUM] X-Content-Type-Options: El servidor no previene el sniffing de tipos MIME, lo que podría permitir que archivos cargados sean interpretados de forma maliciosa.
[MEDIUM] Referrer-Policy: No hay control sobre la información de navegación que se envía a sitios terceros a través de la cabecera Referer.
[MEDIUM] Permissions-Policy: Falta una política que restrinja el acceso de las APIs del navegador a funciones sensibles como cámara o micrófono.
[LOW] Server header expuesto: El encabezado revela que el sistema utiliza nginx/1.24.0 sobre Ubuntu, facilitando a los atacantes la búsqueda de vulnerabilidades específicas.
[LOW] SSL/TLS - Caducidad: El certificado de seguridad actual expira en solo 28 días, lo que representa un riesgo de interrupción de servicio a corto plazo.
[LOW] Robots.txt y Sitemap: No se encontraron estos archivos (Error 404), lo cual afecta la indexación y el control de acceso de rastreadores automáticos.