EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.yape.com.pe/	Checks	9 pruebas
Dominio	www.yape.com.pe	Hallazgos	55 totales
Fecha	8 de abril de 2026 a las 14:28	Problemas	9 detectados

B

87/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha arrojado una puntuación de 87/100, lo que equivale a una nota de B. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 6 verificaciones exitosas, 2 advertencias y 1 fallo crítico relacionado con la exposición de infraestructura. A pesar de contar con una excelente configuración de cifrado y cabeceras, la presencia de múltiples puertos de administración y bases de datos abiertos representa un riesgo significativo. Se concluye que el sitio es vulnerable a nivel de infraestructura, requiriendo intervención inmediata en la configuración del cortafuegos. El estado actual permite una navegación segura para el usuario, pero expone servicios críticos que podrían ser explotados por atacantes externos.

Resumen de Riesgos

3	4	2	0	46
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 123 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	67	AVISO	dtCookie: falta HttpOnly; dtCookie: falta Secure...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	20	FALLO	5 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 123 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  123 dias restantes (expira: 2026-08-09T23:31:01.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-07-08T23:31:02.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' 'unsafe-inline' *.cookiebot.com https://st...

- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin, strict-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(), camera=(), microphone=(), encrypted-media=(), autoplay=(), fulls...

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.yape.com.pe/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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**
  React, 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 — 67/100

Estado: AVISO

dtCookie: falta HttpOnly; dtCookie: falta Secure; dtCookie: falta SameSite; incap_ses_536_2433488: falta HttpOnly

- INFO **Cookies detectadas**
  4 cookie(s) encontrada(s)
- ALTO **Cookie: dtCookie — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: dtCookie — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: dtCookie — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: visid_incap_2433488 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: visid_incap_2433488 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: visid_incap_2433488 — SameSite**
  SameSite=none
- INFO **Cookie: nlbi_2433488 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: nlbi_2433488 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: nlbi_2433488 — SameSite**
  SameSite=none
- ALTO **Cookie: incap_ses_536_2433488 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: incap_ses_536_2433488 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: incap_ses_536_2433488 — SameSite**
  SameSite=none

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 robots.txt

- INFO **sitemap.xml**
  Presente, 286 URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

5 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3389 (RDP)**
  ABIERTO — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- CRITICO **Puerto 6379 (Redis)**
  ABIERTO — Cache Redis sin autenticacion por defecto
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Puerto 3306 (MySQL): El servicio de base de datos está expuesto a internet, lo que permite intentos de fuerza bruta y posibles fugas de información.
[CRITICAL] Puerto 3389 (RDP): El servicio de escritorio remoto de Windows está abierto, siendo un vector principal para ataques de Ransomware y acceso no autorizado.
[CRITICAL] Puerto 6379 (Redis): La caché Redis es accesible externamente y suele carecer de autenticación por defecto, exponiendo datos temporales de la sesión o aplicación.
[HIGH] Puerto 21 (FTP): Protocolo de transferencia de archivos sin cifrar que permite la interceptación de credenciales y datos en tránsito.
[HIGH] Cookie dtCookie (HttpOnly/Secure): La falta de estos flags permite que la cookie sea accesible mediante scripts maliciosos y sea enviada por canales no seguros, aumentando el riesgo de ataques XSS.
[HIGH] Cookie incap_ses_536_2433488 (HttpOnly): Al carecer del flag HttpOnly, la sesión es vulnerable a ser robada mediante vulnerabilidades de Cross-Site Scripting.
[MEDIUM] Cookie dtCookie (SameSite): La ausencia de este atributo facilita la ejecución de ataques de falsificación de solicitudes entre sitios o CSRF.
[MEDIUM] Puerto 8080 (HTTP-Alt): Servidor web alternativo o panel de administración expuesto que amplía la superficie de ataque del servidor.
[LOW] Falta de robots.txt: La ausencia de este archivo impide dar instrucciones claras a los rastreadores sobre qué áreas del sitio no deben ser indexadas.