EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Drtcjunin.gob.pe	Checks	9 pruebas
Dominio	drtcjunin.gob.pe	Hallazgos	48 totales
Fecha	2 de mayo de 2026 a las 05:30	Problemas	19 detectados

D

52/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica del sitio web ha resultado en una puntuación de 52/100, lo que equivale a una calificación de grado D. Durante la evaluación se ejecutaron 9 checks pasivos, identificando 3 resultados satisfactorios, 2 advertencias y 4 fallos críticos en la configuración. La presencia de software desactualizado y la ausencia total de cabeceras de protección básicas representan un riesgo significativo para la integridad del portal. Debido a estas deficiencias estructurales y a la exposición de servicios críticos, se concluye que el sitio es actualmente vulnerable a ataques externos.

Resumen de Riesgos

0	6	9	4	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 59 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, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.9.4 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	11 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 59 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  59 dias restantes (expira: 2026-06-30T02:33:47.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-01T02:33:48.000Z
- 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: Apache — 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://drtcjunin.gob.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: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  Next.js, Astro

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta

- ALTO **WordPress version**
  Version 6.9.4 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 20/100

Estado: FALLO

11 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://drtcjunin.gob.pe/circulacion/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://drtcjunin.gob.pe/circulacion/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://drtcjunin.gob.pe/infraestructura/
- MEDIO **href (link/stylesheet)**
  ...y 8 mas del mismo tipo

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

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- 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: Falta — La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: Falta — El sitio es vulnerable a ataques de clickjacking al permitir que el contenido se cargue en marcos externos.
[HIGH] Strict-Transport-Security: Falta — No se fuerza el uso de HTTPS, lo que permite ataques de degradación de protocolo (SSL Stripping).
[HIGH] WordPress version: 6.9.4 expuesta — El uso de una versión obsoleta permite a atacantes explotar vulnerabilidades conocidas y documentadas (CVEs).
[HIGH] Puerto 21 (FTP): ABIERTO — Este servicio transmite datos y credenciales en texto plano, siendo altamente inseguro.
[MEDIUM] X-Content-Type-Options: Falta — Permite que el navegador realice sniffing de tipos MIME, lo que facilita la ejecución de scripts camuflados.
[MEDIUM] Referrer-Policy: Falta — No se controla la información de navegación que se envía a otros dominios, comprometiendo la privacidad de los usuarios.
[MEDIUM] Permissions-Policy: Falta — No se restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Contenido Mixto: 11 recursos HTTP — Se detectaron elementos que se cargan sin cifrar dentro de la página segura, debilitando la protección SSL.
[MEDIUM] Ruta /wp-login.php: Expuesta — El acceso público al panel de administración facilita ataques de fuerza bruta contra las credenciales.
[MEDIUM] Puerto 22 (SSH): ABIERTO — Mantiene un vector de acceso remoto que debe ser monitoreado y protegido estrictamente.
[LOW] Server header: Apache expuesto — Revela la tecnología del servidor, ayudando a los atacantes a realizar un reconocimiento más preciso.
[LOW] Meta generator: WordPress 6.9.4 — Expone innecesariamente la versión del CMS en el código fuente.
[LOW] Archivos faltantes: robots.txt y sitemap.xml — No se encontraron estos archivos, lo que afecta el control de rastreo y la indexación profesional.