EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ija.edu.pa	Checks	9 pruebas
Dominio	ija.edu.pa	Hallazgos	50 totales
Fecha	22 de abril de 2026 a las 14:41	Problemas	19 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 57/100, lo que corresponde a una calificación de grado D. Durante la auditoría se ejecutaron 9 checks pasivos, resultando en 4 aprobados, 1 advertencia y 4 fallos críticos en la configuración. La presencia de múltiples vulnerabilidades de severidad alta y la exposición de servicios internos representan un riesgo significativo para la integridad de la plataforma. Debido a la falta de cabeceras de seguridad y al uso de software desactualizado, se concluye que el sitio es actualmente vulnerable a diversos vectores de ataque.

Resumen de Riesgos

1	5	11	2	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 64 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
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, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	39 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 64 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  64 dias restantes (expira: 2026-06-25T21:24:58.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-27T21:24:59.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- 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://ija.edu.pa/
- 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

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.9.4 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- 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

39 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://ija.edu.pa/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.instagram.com/ijapma
- MEDIO **href (link/stylesheet)**
  ...y 35 mas del mismo tipo
- MEDIO **Recurso HTTP (CSS url())**
  http://ija.edu.pa/wp-content/uploads/2017/05/barra4.jpg

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (168 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://ija.edu.pa/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- 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
- 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 está expuesta directamente a internet, permitiendo intentos de acceso no autorizado y robo de información.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos abierto sin cifrado, lo que facilita la interceptación de credenciales de administración.
[HIGH] Versión de WordPress expuesta (6.9.4): El sistema utiliza una versión obsoleta que permite a atacantes explotar vulnerabilidades conocidas públicamente.
[HIGH] X-Frame-Options: La falta de esta cabecera hace que el sitio sea susceptible a ataques de clickjacking para engañar a los usuarios.
[HIGH] Strict-Transport-Security: La ausencia de HSTS no obliga al navegador a usar conexiones seguras, permitiendo ataques de degradación de protocolo.
[MEDIUM] Contenido Mixto: Se detectaron 39 recursos cargados vía HTTP dentro de la página HTTPS, lo que compromete la privacidad de la navegación.
[MEDIUM] Puerto 22 (SSH): El puerto de administración remota está abierto, incrementando la superficie de ataque para intentos de fuerza bruta.
[MEDIUM] X-Content-Type-Options: Falta de protección contra el sniffing de tipos MIME, lo que podría derivar en la ejecución de scripts maliciosos.
[MEDIUM] Ruta /wp-login.php y /readme.html: El panel de acceso y archivos informativos están expuestos, facilitando el reconocimiento por parte de atacantes.
[MEDIUM] Referrer-Policy y Permissions-Policy: Ausencia de políticas para controlar la información enviada a terceros y restringir el uso de APIs del navegador.
[LOW] Server header expuesto: El servidor revela el uso de Apache, proporcionando información técnica valiosa para un atacante.
[LOW] Meta generator: Se expone públicamente en el código fuente el uso de WordPress 6.9.4.