EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://unipaz.edu.co/	Checks	9 pruebas
Dominio	unipaz.edu.co	Hallazgos	40 totales
Fecha	5 de septiembre de 2026 a las 20:27	Problemas	6 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al portal institucional ha arrojado una puntuación de 85/100 con una calificación de nota B. Se ejecutaron un total de 9 checks pasivos, resultando en 4 verificaciones exitosas y 3 advertencias, sin detectar fallos críticos de seguridad inmediatos. El análisis revela una base técnica estable, pero con deficiencias en la configuración de privacidad de cabeceras y gestión de puertos. En conclusión, el sitio web se considera moderadamente seguro, aunque vulnerable a tácticas de reconocimiento debido a la exposición de información técnica del servidor.

Resumen de Riesgos

0	0	3	3	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 51 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: Permissions-Policy
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 51 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  51 dias restantes (expira: 2026-10-26T14:57:27.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-28T13:59:51.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor
- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.1.34 — Revela framework/lenguaje

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=0
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

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: Elementor 3.33.0; features: additional_custom_breakpoints; settings: css_print_method-internal, google_font-enabled, font_display-swap
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.1.34

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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://unipaz.uxxi.com/pagosenLinea_prod/index.jsp

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (171 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow

- INFO **Sitemap en robots.txt**
  https://unipaz.edu.co/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- 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
- 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

[MEDIUM] Permissions-Policy faltante: La ausencia de esta cabecera impide restringir el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[MEDIUM] Contenido mixto detectado: Se identificó un recurso de la pasarela de pagos (unipaz.uxxi.com) cargando mediante el protocolo inseguro HTTP, lo que compromete la integridad de la conexión cifrada.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este puerto alternativo puede ser utilizada para acceder a servicios de administración o proxies no protegidos adecuadamente.
[LOW] Cabecera de servidor expuesta: El sistema revela el uso de Cloudflare como tecnología de servidor, facilitando el perfilamiento del sitio por parte de atacantes.
[LOW] X-Powered-By expuesto: Se detectó la divulgación de la versión específica PHP/8.1.34, lo que permite la búsqueda dirigida de exploits para esa versión.
[LOW] Meta generator expuesto: La etiqueta revela el uso de Elementor 3.33.0 y configuraciones internas de WordPress, exponiendo la superficie de ataque del CMS.