EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://unpaz.edu.ar	Checks	9 pruebas
Dominio	unpaz.edu.ar	Hallazgos	54 totales
Fecha	7 de mayo de 2026 a las 07:17	Problemas	13 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el dominio unpaz.edu.ar ha resultado en una puntuación de 85/100, lo que equivale a una calificación de nota B. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 fue clasificado como fallo. El sitio demuestra una implementación sólida de certificados SSL y protocolos de redirección HTTPS, garantizando la privacidad de la conexión inicial. Sin embargo, la presencia de contenido mixto y la ausencia de políticas de seguridad de contenido exponen vectores de ataque conocidos. Se concluye que el sitio es mayormente seguro, pero presenta vulnerabilidades moderadas que requieren atención inmediata para prevenir ataques de inyección.

Resumen de Riesgos

0	1	6	6	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 39 dias
Cabeceras de Seguridad	75	AVISO	5/6 presentes. Faltan: Content-Security-Policy
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: Drupal
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	4 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 39 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  39 dias restantes (expira: 2026-06-15T16:37:31.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-17T16:37:32.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

5/6 presentes. Faltan: Content-Security-Policy

- BAJO **Server header expuesto**
  Server: Apache/2.4.62 (Debian) — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.24 — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(), microphone=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://unpaz.edu.ar/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Drupal

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  Detectado via HTML body
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Drupal 10 (https://www.drupal.org)
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.3.24

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

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

4 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://cjys.unpaz.edu.ar/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://csyd.unpaz.edu.ar/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://conusur.unaj.edu.ar/el-consorcio-conusur/
- MEDIO **href (link/stylesheet)**
  ...y 1 mas del mismo tipo

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (2027 bytes)
- INFO **Reglas robots.txt**
  34 Disallow, 18 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web

- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) y otros tipos de inyección de contenido malicioso.
[MEDIUM] Contenido Mixto: Se detectaron 4 recursos (stylesheets y links) cargados a través de HTTP, lo que compromete la integridad de la página cifrada.
[MEDIUM] Archivo README.txt: Este archivo es accesible de forma pública, lo que facilita a un atacante obtener información técnica sobre la instalación de Drupal.
[MEDIUM] Panel de Login Expuesto: La ruta /user/login se encuentra disponible para acceso público, aumentando el riesgo de ataques de fuerza bruta dirigidos.
[LOW] Cabecera Server Expuesta: El servidor revela el uso de Apache/2.4.62 (Debian), lo que permite a atacantes buscar exploits específicos para esa versión.
[LOW] Cabecera X-Powered-By: Se expone el uso de PHP/8.3.24, revelando información sobre el stack tecnológico subyacente.
[LOW] Etiqueta Meta Generator: El código fuente del sitio confirma el uso de Drupal 10, lo que reduce el esfuerzo de reconocimiento para un atacante.
[LOW] Rutas Sensibles en Robots.txt: El archivo menciona directorios como admin y config, proporcionando un mapa de áreas críticas a usuarios no autorizados.
[LOW] Ausencia de Sitemap: No se localizó el archivo sitemap.xml, lo que puede afectar la auditoría de rutas y la indexación controlada del sitio.