EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://utp.ac.pa	Checks	9 pruebas
Dominio	utp.ac.pa	Hallazgos	47 totales
Fecha	25 de abril de 2026 a las 01:44	Problemas	13 detectados

B

75/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación técnica de 75/100, lo que representa una nota de calificación B. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 5 resultaron exitosos, uno generó una advertencia y dos presentaron fallos críticos de configuración. Si bien el sitio posee un cifrado de transporte robusto, se han detectado debilidades importantes en las cabeceras de seguridad y la exposición de servicios en puertos no estándar. Se concluye que el sitio es moderadamente vulnerable, requiriendo ajustes técnicos inmediatos para mitigar riesgos de interceptación y ataques de intermediario.

Resumen de Riesgos

0	1	9	3	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 50 dias
Cabeceras de Seguridad	55	FALLO	Solo 3/6 presentes. Faltan: Strict-Transport-Sec...
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	6 recursos 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 50 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  50 dias restantes (expira: 2026-06-13T20:37:01.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-15T19:37:04.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor
- INFO **Content-Security-Policy**
  Presente: frame-ancestors 'self' https://sostenible.utp.ac.pa

- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff, nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

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 7 (https://www.drupal.org)
- INFO **Tecnologias detectadas**
  Next.js

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

6 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.ridda2.utp.ac.pa/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://centrodelenguas.utp.ac.pa/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.sistemadebibliotecas.utp.ac.pa/
- MEDIO **href (link/stylesheet)**
  ...y 3 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (2189 bytes)
- INFO **Reglas robots.txt**
  36 Disallow, 32 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **sitemap.xml**
  Presente, 16 URLs
- 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

[HIGH] Strict-Transport-Security: Falta esta cabecera esencial que obliga al navegador a usar siempre conexiones seguras, previniendo ataques de degradación de protocolo.
[MEDIUM] Contenido Mixto: Se detectaron 6 recursos cargados mediante HTTP (como hojas de estilo de subdominios ridda2, centrodelenguas y sistemadebibliotecas) dentro de la página HTTPS, lo que compromete la integridad del sitio.

[MEDIUM] Puerto 8080 (HTTP-Alt) Abierto: La exposición de un servidor web alternativo o proxy aumenta la superficie de ataque y puede ser explotado si no está debidamente asegurado.
[MEDIUM] Referrer-Policy: La ausencia de esta cabecera impide controlar qué información de navegación se envía a terceros cuando se hace clic en un enlace.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[MEDIUM] Archivo /README.txt accesible: Este archivo público revela que el sitio utiliza Drupal y puede exponer detalles sobre la arquitectura interna.
[MEDIUM] Ruta /user/login accesible: El punto de acceso administrativo está expuesto a internet, facilitando intentos de acceso no autorizado mediante fuerza bruta.
[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando información útil a un atacante sobre la infraestructura de red.
[LOW] Meta generator expuesto: El código fuente indica explícitamente el uso de Drupal 7, permitiendo a un atacante buscar vulnerabilidades específicas para esa versión.
[LOW] Ruta sensible en robots.txt: El archivo menciona la ruta admin, lo que ayuda a un atacante a mapear directorios restringidos del servidor.