EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://matricula.utp.ac.pa/Session/Cuenta/Validar/lUe0V0gUdP$QjSioRkmTniiTTQ$	Pruebas	9 pruebas
Dominio	matricula.utp.ac.pa	Hallazgos	48 totales
Fecha	25 de abril de 2026 a las 01:47	Problemas	19 detectados

D

54/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 54/100, lo que equivale a una calificación de grado D. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo 3 resultados satisfactorios, 2 advertencias y 3 fallos críticos en la configuración. A pesar de contar con un cifrado de transporte válido, la ausencia de protecciones básicas contra ataques de inyección y el uso de recursos no seguros comprometen la integridad de la sesión. Se concluye que el sitio es actualmente vulnerable y requiere intervenciones inmediatas para mitigar riesgos de seguridad.

Resumen de Riesgos

0	3	14	2	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 50 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	67	AVISO	__AntiXsrfToken: falta SameSite
Contenido Mixto	20	FALLO	6 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
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 — 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: cloudflare — Revela tecnologia del servidor
- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — Revela framework/lenguaje

- 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.)

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  ASP.NET

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

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

Seguridad de Cookies — 67/100

Estado: AVISO

__AntiXsrfToken: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)

- INFO **Cookie: __AntiXsrfToken — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __AntiXsrfToken — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: __AntiXsrfToken — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 20/100

Estado: FALLO

6 recursos HTTP en pagina HTTPS

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

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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] Content-Security-Policy: Falta esta cabecera esencial para prevenir ataques de ejecución de scripts cruzados (XSS) e inyecciones de contenido.

[HIGH] X-Frame-Options: La ausencia de esta protección hace que el sitio sea vulnerable a ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, permitiendo posibles degradaciones de seguridad en la conexión.
[MEDIUM] Contenido Mixto: Se detectaron 6 recursos cargados mediante HTTP en una página HTTPS, lo que expone al usuario a ataques de interceptación de datos.
[MEDIUM] Cookie AntiXsrfToken: El token de seguridad carece del atributo SameSite, facilitando la ejecución de ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Archivos Informativos Expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente y pueden revelar detalles técnicos del servidor.
[MEDIUM] Paneles de Login Expuestos: Se detectó acceso público a rutas críticas como /wp-login.php, /administrator/ y /user/login, aumentando el riesgo de ataques de fuerza bruta.
[MEDIUM] Puerto 8080 Abierto: La presencia del puerto HTTP-Alt activo representa un vector de ataque adicional si no está restringido correctamente.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido, facilitando ataques de MIME-sniffing.
[MEDIUM] Referrer-Policy y Permissions-Policy: Ausencia de controles sobre la información de procedencia y el uso de APIs del navegador como cámara o micrófono.
[LOW] Exposición de Tecnologías: Las cabeceras del servidor revelan explícitamente el uso de Cloudflare y el framework ASP.NET, facilitando el reconocimiento a atacantes.