EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.tecazuay.edu.ec/	Checks	9 pruebas
Dominio	www.tecazuay.edu.ec	Hallazgos	50 totales
Fecha	19 de mayo de 2026 a las 00:49	Problemas	13 detectados

C

67/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 67/100, obteniendo una calificación de nota C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 3 generaron advertencias y 2 fueron identificados como fallos críticos. Se han detectado debilidades significativas en la configuración de cabeceras de seguridad, exposición de versiones de software y servicios de red inseguros. Debido a la combinación de vulnerabilidades de severidad alta y la falta de mecanismos de protección modernos, se concluye que el sitio es actualmente vulnerable ante ataques de inyección y accesos no autorizados.

Resumen de Riesgos

0	5	5	3	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 47 dias
Cabeceras de Seguridad	55	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
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
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	4 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): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 47 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  47 dias restantes (expira: 2026-07-04T18:30:43.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-05T18:30:44.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(), microphone=(), camera=()

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.tecazuay.edu.ec/
- 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

- ALTO **WordPress version**
  Version 6.9.4 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- 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

4 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://200.24.148.68:10030/sys_evaluacion_ista/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://200.24.148.68:10030/sys_evaluacion_ista/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.registrounicoedusup.gob.ec
- MEDIO **href (link/stylesheet)**
  ...y 1 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (120 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.tecazuay.edu.ec/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- 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: Falta esta cabecera esencial, lo que permite la ejecución de ataques XSS y la inyección de contenido malicioso.
[HIGH] Strict-Transport-Security: La ausencia de HSTS impide que el navegador fuerce conexiones HTTPS, dejando a los usuarios expuestos a ataques de degradación de protocolo.
[HIGH] WordPress version: Se expone públicamente la versión 6.9.4 del CMS, lo que permite a atacantes identificar y explotar CVEs conocidos para esta versión específica.
[HIGH] Puerto 21 (FTP): El puerto se encuentra abierto, lo cual es peligroso ya que el protocolo FTP transmite credenciales y archivos sin cifrar.
[MEDIUM] Contenido Mixto: Se detectaron 4 recursos cargados mediante HTTP (incluyendo enlaces a 200.24.148.68 y registrounicoedusup.gob.ec), lo que compromete la integridad de la conexión cifrada.
[MEDIUM] Ruta /wp-login.php: El panel de administración de WordPress es accesible de forma pública, facilitando ataques de fuerza bruta contra las credenciales institucionales.
[LOW] Server header expuesto: La cabecera del servidor revela el uso de LiteSpeed, proporcionando información técnica innecesaria a potenciales atacantes.
[LOW] Meta generator: El código fuente expone la etiqueta WordPress 6.9.4, confirmando la tecnología y versión utilizada.
[LOW] Ruta sensible en robots.txt: El archivo de directivas para buscadores incluye una referencia al directorio admin, revelando rutas privadas de la estructura web.