

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://utp.edu.pe	Checks	9 pruebas
Dominio	utp.edu.pe	Hallazgos	49 totales
Fecha	8 de septiembre de 2026 a las 02:44	Problemas	7 detectados

A

90/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio utp.edu.pe arroja una puntuación de 90/100 con una nota final de A. Se ejecutaron un total de 9 checks pasivos, de los cuales 8 resultaron satisfactorios y únicamente 1 presentó fallos críticos relacionados con las cabeceras de respuesta. A pesar de la ausencia de un pentest activo, la configuración de cifrado y redirección de tráfico es excelente. Se concluye que el sitio es generalmente seguro, aunque presenta vectores de riesgo específicos por la falta de políticas de seguridad en el navegador.

Resumen de Riesgos

0	1	2	4	42
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 130 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: Drupal, PrestaShop
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 130 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
130 dias restantes (expira: 2027-01-15T16:09:59.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-07-01T16:09:59.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

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

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

- 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=31536000; includeSubDomains; preload
- INFO

X-Content-Type-Options
Presente: nosniff
- MEDIO

Referrer-Policy
Falta — Controla la informacion de referer enviada
- MEDIO

Permissions-Policy
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://utp.edu.pe:443/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO

HSTS includeSubDomains
HSTS cubre subdominios
- INFO

HSTS max-age
max-age=31536000 (365 dias)
- INFO

Respuesta HTTPS
HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Drupal, PrestaShop

- INFO

WordPress
No detectado
- INFO

Joomla
No detectado
- INFO

Drupal
Detectado via HTML body
- 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: Drupal 10 (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)

- INFO

Archivo /README.txt
No accesible (correcto)
- 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 — 100/100

Estado: OK

No se detecto contenido mixto

- INFO

Contenido mixto
Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- 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
- INFO

sitemap.xml
Presente, ? URLs
- BAJO

security.txt
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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



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 la ejecución de scripts no autorizados, aumentando el riesgo de ataques XSS e inyección de contenido malicioso.

[MEDIUM] Referrer-Policy: No se encuentra configurada, lo que podría exponer información sensible de la navegación de los usuarios a dominios de terceros.

[MEDIUM] Permissions-Policy: Falta esta política para restringir el acceso de las APIs del navegador a componentes de hardware como cámara, micrófono o geolocalización.

[LOW] Server header expuesto: El servidor responde con la cabecera Server: nginx, facilitando a un atacante el reconocimiento de la tecnología base para buscar exploits específicos.

[LOW] Meta generator: La etiqueta revela el uso de Drupal 10, lo cual expone la arquitectura del CMS y permite ataques dirigidos a vulnerabilidades conocidas de dicha versión.

[LOW] Rutas sensibles en robots.txt: Se identificaron referencias directas a rutas como admin y config, lo que ayuda a potenciales atacantes a mapear áreas administrativas restringidas.