EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://nube.utesa.edu/	Checks	9 pruebas
Dominio	nube.utesa.edu	Hallazgos	47 totales
Fecha	27 de mayo de 2026 a las 19:26	Problemas	11 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el dominio arroja una puntuación de 72/100, lo que resulta en una calificación de grado C. Durante la evaluación se ejecutaron un total de 9 checks pasivos, obteniendo 6 resultados satisfactorios, 1 advertencia y 2 fallos críticos relacionados con la configuración del servidor. El sitio web carece de todas las cabeceras de seguridad esenciales para proteger a los usuarios finales frente a ataques modernos. En su estado actual, el sitio se considera vulnerable a ataques de inyección, clickjacking y divulgación de información técnica sensible.

Resumen de Riesgos

0	4	3	4	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 74 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	100	OK	1 cookies, todas con flags correctos
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 74 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  74 dias restantes (expira: 2026-08-10T04:43:10.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-12T04:43:11.000Z
- 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: Apache/2.4.62 (Debian) — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.4.12 — 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.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 308 redirige a https://nube.utesa.edu/
- 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

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**
  PHP/8.4.12

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

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: MoodleSession — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: MoodleSession — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: MoodleSession — SameSite**
  SameSite=lax

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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, facilitando ataques de Cross-Site Scripting (XSS) e inyección de datos.
[HIGH] X-Frame-Options: Falta de protección contra ataques de clickjacking, lo que permitiría a un atacante cargar el sitio en marcos invisibles para engañar a los usuarios.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que permite que la conexión sea degradada de HTTPS a HTTP mediante ataques de tipo interceptación.
[MEDIUM] X-Content-Type-Options: El servidor no previene el rastreo de tipos MIME, permitiendo que el navegador interprete archivos de forma incorrecta y ejecute código malicioso.
[MEDIUM] Referrer-Policy: No hay control sobre la información de referencia enviada a otros dominios, lo que puede filtrar URLs privadas a sitios de terceros.
[MEDIUM] Permissions-Policy: La falta de esta política permite que el sitio acceda innecesariamente a APIs del navegador como la cámara, el micrófono o la geolocalización.
[LOW] Server header expuesto: El servidor revela el uso de Apache/2.4.62 (Debian), lo que permite a un atacante buscar vulnerabilidades específicas para esa versión exacta.
[LOW] X-Powered-By expuesto: Se divulga el uso de PHP/8.4.12, proporcionando detalles sobre el lenguaje de programación y su versión para facilitar ataques dirigidos.
[LOW] Ausencia de robots.txt y sitemap.xml: La inexistencia de estos archivos dificulta el control de los rastreadores y la indexación correcta de la estructura del sitio.