EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://amfs.tec.mx/nidp/saml2/sso?id=itesmauth-identidadsl2pu&sid=2&option=credentialsbas	Opciones	9 habilitadas=2
Dominio	amfs.tec.mx	Hallazgos	56 totales
Fecha	16 de julio de 2026 a las 04:42	Problemas	13 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja una puntuación de 76/100 con una calificación de grado B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 presentó advertencias y 3 fueron calificados como fallos. Aunque la capa de cifrado y transporte de datos es robusta, se detectaron deficiencias críticas en la configuración de puertos y cabeceras de seguridad. En conclusión, el sitio se considera vulnerable debido a la exposición de servicios internos que podrían ser explotados por atacantes externos.

Resumen de Riesgos

3	3	5	2	43
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 125 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	75	AVISO	JSESSIONID: falta SameSite; UrnNovellNidpCluster...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	20	FALLO	5 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 125 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  125 dias restantes (expira: 2026-11-17T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-10-23T00:00:00.000Z
- 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

- 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
- 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://amfs.tec.mx/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no 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

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**
  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 — 75/100

Estado: AVISO

JSESSIONID: falta SameSite; UrnNovellNidpClusterMemberId: falta SameSite; incap_ses_612_2928281: falta HttpOnly

- INFO **Cookies detectadas**
  4 cookie(s) encontrada(s)
- INFO **Cookie: JSESSIONID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: JSESSIONID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: JSESSIONID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: UrnNovellNidpClusterMemberId — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: UrnNovellNidpClusterMemberId — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: UrnNovellNidpClusterMemberId — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: visid_incap_2928281 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: visid_incap_2928281 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: visid_incap_2928281 — SameSite**
  SameSite=none
- ALTO **Cookie: incap_ses_612_2928281 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: incap_ses_612_2928281 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: incap_ses_612_2928281 — SameSite**
  SameSite=none

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 — 20/100

Estado: FALLO

5 puertos riesgosos abiertos

- 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- CRITICO **Puerto 3389 (RDP)**
  ABIERTO — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- CRITICO **Puerto 6379 (Redis)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL): Base de datos expuesta directamente a internet, permitiendo intentos de acceso no autorizados y ataques de fuerza bruta.
[CRITICAL] Puerto 3389 (RDP): Interfaz de escritorio remoto de Windows abierta, facilitando el secuestro de sesiones o explotación de vulnerabilidades del protocolo.
[CRITICAL] Puerto 6379 (Redis): Servicio de caché expuesto que habitualmente carece de autenticación, arriesgando la integridad y confidencialidad de los datos temporales.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] Puerto 21 (FTP): Protocolo de transferencia de archivos activo sin cifrado, lo que permite la interceptación de credenciales y datos en tránsito.
[HIGH] Cookie incap_ses_612_2928281: Carece del atributo HttpOnly, permitiendo que scripts maliciosos accedan a la cookie y roben la sesión del usuario.
[MEDIUM] Puerto 8080 (HTTP-Alt): Servidor web alternativo expuesto que incrementa la superficie de ataque del servidor.
[MEDIUM] Referrer-Policy: Falta de control sobre la información de procedencia enviada en las peticiones, lo que puede filtrar URLs sensibles.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs del navegador, dejando activos componentes como cámara o micrófono innecesariamente.
[MEDIUM] Cookie JSESSIONID: Falta el atributo SameSite, lo que hace al usuario vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Cookie UrnNovellNidpClusterMemberId: Ausencia de atributo SameSite, permitiendo posibles vectores de ataque de tipo CSRF.
[LOW] robots.txt y sitemap.xml: Archivos de configuración no encontrados, dificultando la gestión del rastreo por motores de búsqueda.