EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://mitec.itesm.mx/Paginas/mitec/index.aspx#/https://mitec.itesm.mx/Paginas/mitec/index.aspx#/	Checks	9 ejecutados
Dominio	mitec.itesm.mx	Hallazgos	52 totales
Fecha	16 de julio de 2026 a las 05:00	Problemas	12 detectados

B

81/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al dominio mitec.itesm.mx arrojó una puntuación de 81/100, lo que corresponde a una calificación de B. Se ejecutaron 9 verificaciones pasivas, de las cuales 5 resultaron satisfactorias, 2 generaron advertencias y 2 fueron marcadas como fallos críticos. Aunque la comunicación cifrada mediante SSL es sólida, se detectaron brechas graves en la configuración de la infraestructura y puertos del servidor. En su estado actual, el sitio se considera vulnerable debido a la exposición pública de servicios críticos de base de datos y administración remota.

Resumen de Riesgos

3	2	3	4	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 142 dias
Cabeceras de Seguridad	75	AVISO	4/6 presentes. Faltan: Referrer-Policy, Permissi...
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	83	AVISO	incap_ses_612_2325189: falta HttpOnly
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 142 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  142 dias restantes (expira: 2026-12-04T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-20T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

4/6 presentes. Faltan: Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Microsoft-IIS/10.0 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: frame-ancestors 'self' teams.microsoft.com *.teams.microsoft.com *.skype.com *.t...
- 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://mitec.itesm.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 403

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

- 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 — 83/100

Estado: AVISO

incap_ses_612_2325189: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: visid_incap_2325189 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: visid_incap_2325189 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: visid_incap_2325189 — SameSite**
  SameSite=none
- ALTO **Cookie: incap_ses_612_2325189 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: incap_ses_612_2325189 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: incap_ses_612_2325189 — 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): Servicio de base de datos expuesto directamente a internet, permitiendo intentos de intrusión externa.
[CRITICAL] Puerto 3389 (RDP): Escritorio remoto de Windows abierto, lo que facilita ataques de fuerza bruta para tomar control del servidor.
[CRITICAL] Puerto 6379 (Redis): Instancia de caché expuesta que usualmente carece de autenticación, arriesgando la fuga de datos en memoria.
[HIGH] Puerto 21 (FTP): Protocolo de transferencia de archivos sin cifrar habilitado, permitiendo la intercepción de credenciales.
[HIGH] Cookie incap_ses_612_2325189: Falta el atributo HttpOnly, lo que permite que la cookie sea accesible mediante scripts, aumentando el riesgo de ataques XSS.
[MEDIUM] Puerto 8080 (HTTP-Alt): Puerto alternativo abierto que podría exponer servicios internos o interfaces de administración no protegidas.
[MEDIUM] Referrer-Policy: Cabecera ausente, lo que provoca que el sitio no controle cuánta información de navegación se envía a otros dominios.
[MEDIUM] Permissions-Policy: Cabecera ausente, permitiendo que el navegador acceda a funciones sensibles del hardware sin restricciones definidas.
[LOW] Server header expuesto: El servidor revela el uso de Microsoft-IIS/10.0, facilitando a los atacantes la búsqueda de vulnerabilidades específicas para esa versión.
[LOW] X-Powered-By expuesto: Se revela que el sitio utiliza el framework ASP.NET, proporcionando información técnica innecesaria a terceros.
[LOW] robots.txt y sitemap.xml: La ausencia de estos archivos dificulta la gestión de rutas permitidas y el indexado correcto del sitio.