EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://actas.ujat.mx/Account/Login?ReturnUrl=%2f	Checks	9 pruebas
Dominio	actas.ujat.mx	Hallazgos	57 totales
Fecha	7 de agosto de 2026 a las 03:42	Problemas	3 detectados

A

97/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado ha otorgado al sitio una puntuación exacta de 97/100, lo que representa una nota A. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo 7 resultados satisfactorios, 2 advertencias y 0 fallos críticos. La infraestructura analizada demuestra una implementación robusta de protocolos de cifrado y cabeceras de seguridad. En conclusión, el sitio web se considera seguro para su uso operativo, aunque requiere de ajustes menores en la configuración de cookies y archivos de indexación para alcanzar la excelencia técnica.

Resumen de Riesgos

0	0	2	1	54
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 49 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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	92	AVISO	__RequestVerificationToken: falta SameSite
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 49 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  49 dias restantes (expira: 2026-09-24T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-10-15T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- INFO **Content-Security-Policy**
  Presente: default-src 'none'; connect-src 'self'; font-src 'self'; form-action 'self'; fra...

- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer
- INFO **Permissions-Policy**
  Presente: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), micr...

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://actas.ujat.mx/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 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

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 — 92/100

Estado: AVISO

__RequestVerificationToken: falta SameSite

- INFO **Cookies detectadas**
  4 cookie(s) encontrada(s)
- INFO **Cookie: __Secure-SessionId-actas — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __Secure-SessionId-actas — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __Secure-SessionId-actas — SameSite**
  SameSite=strict
- INFO **Cookie: __Secure-SessionId-actas — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __Secure-SessionId-actas — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __Secure-SessionId-actas — SameSite**
  SameSite=strict
- INFO **Cookie: __Secure-SessionId-actas — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __Secure-SessionId-actas — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __Secure-SessionId-actas — SameSite**
  SameSite=strict
- INFO **Cookie: __RequestVerificationToken — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __RequestVerificationToken — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: __RequestVerificationToken — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (28 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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

[MEDIA] Cookie __RequestVerificationToken: La falta del atributo SameSite en esta cookie de sesión la hace vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIA] robots.txt: Se ha detectado una directiva de bloqueo total que impide el rastreo legítimo del sitio, lo cual puede afectar la disponibilidad de información en motores de búsqueda.
[BAJA] sitemap.xml: El archivo de mapa del sitio no fue encontrado, lo que dificulta la navegación de los indexadores automáticos y refleja una falta de mantenimiento en los archivos de configuración raíz.