EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.fam.unam.mx	Checks	9 pruebas
Dominio	www.fam.unam.mx	Hallazgos	40 totales
Fecha	13 de abril de 2026 a las 16:21	Problemas	5 detectados

B

86/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado a www.fam.unam.mx arroja una puntuación exacta de 86/100, lo que corresponde a una calificación de grado B. Se ejecutaron 9 comprobaciones pasivas de seguridad, resultando en 5 verificaciones satisfactorias y 2 advertencias técnicas, sin registrarse fallos críticos totales. Los resultados indican una implementación sólida de cifrado y protocolos de transferencia, aunque se identificaron carencias importantes en la configuración de cabeceras de protección avanzada. Concluimos que el sitio web es generalmente seguro para la navegación informativa, pero se clasifica como vulnerable ante ataques específicos de inyección y recolección de información debido a la exposición de metadatos técnicos.

Resumen de Riesgos

0	1	2	2	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 100 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 100 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  100 dias restantes (expira: 2026-07-22T15:06:07.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-06-20T15:06:08.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache — 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
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin, no-referrer
- 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://www.fam.unam.mx/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains
- 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: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- 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: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  Next.js

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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11

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

[HIGH] Content-Security-Policy: La ausencia de esta cabecera impide definir qué fuentes de contenido son confiables, lo que facilita ataques de Cross-Site Scripting (XSS) e inyección.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso de las APIs del navegador a funciones del hardware, como cámara o micrófono, aumentando el riesgo de privacidad para el usuario.
[MEDIUM] Contenido Mixto: Se detectó el recurso http://gmpg.org/xfn/11 cargado mediante protocolo inseguro dentro de una página HTTPS, lo que degrada la integridad de la conexión.
[LOW] Meta generator: El sitio expone públicamente el uso de WordPress 6.9.4, permitiendo a posibles atacantes buscar vulnerabilidades específicas para esa versión del CMS.
[LOW] Server header expuesto: La cabecera del servidor revela el uso de Apache, proporcionando información técnica valiosa a terceros para perfilar vectores de ataque.