EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ivirtual.itson.edu.mx	Checks	9 pruebas
Dominio	ivirtual.itson.edu.mx	Hallazgos	51 totales
Fecha	5 de mayo de 2026 a las 16:47	Problemas	15 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio ivirtual.itson.edu.mx arroja una puntuación de 68/100, lo que resulta en una calificación de grado C. Se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 presentó advertencias y 3 fallaron debido a configuraciones críticas ausentes. Aunque el cifrado de transporte base es correcto, la carencia de cabeceras de protección modernas y la gestión insegura de cookies exponen el sitio a riesgos de interceptación y suplantación de identidad. En conclusión, el sitio se considera vulnerable a ataques dirigidos contra los usuarios finales debido a una superficie de ataque no mitigada en la capa de aplicación.

Resumen de Riesgos

0	7	5	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 50 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 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	33	FALLO	ApplicationGatewayAffinityCORS: 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	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 50 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  50 dias restantes (expira: 2026-06-24T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-06-24T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache/2.4.58 (Ubuntu) — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: sameorigin
- 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 301 redirige a https://ivirtual.itson.edu.mx/
- 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

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 — 33/100

Estado: FALLO

ApplicationGatewayAffinityCORS: falta HttpOnly; ApplicationGatewayAffinity: falta HttpOnly; ApplicationGatewayAffinity: falta Secure; ApplicationGatewayAffinity: falta SameSite; MoodleSession: falta HttpOnly; MoodleSession: falta SameSite

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- ALTO **Cookie: ApplicationGatewayAffinityCORS — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: ApplicationGatewayAffinityCORS — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: ApplicationGatewayAffinityCORS — SameSite**
  SameSite=none
- ALTO **Cookie: ApplicationGatewayAffinity — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: ApplicationGatewayAffinity — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: ApplicationGatewayAffinity — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: MoodleSession — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: MoodleSession — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: MoodleSession — 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 — 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

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 facilita ataques de Cross-Site Scripting (XSS) e inyección de contenido al no restringir los orígenes de carga de scripts.
[HIGH] Strict-Transport-Security: Falta la configuración de HSTS, lo que permite que la conexión sea degradada de HTTPS a HTTP mediante ataques de tipo man-in-the-middle.
[HIGH] Cookie MoodleSession sin HttpOnly: Esta cookie de sesión es accesible mediante JavaScript, permitiendo que un atacante robe la identidad del usuario a través de un script malicioso.
[HIGH] Cookie ApplicationGatewayAffinity sin Secure: La falta de este flag permite que una cookie técnica sea transmitida por canales no cifrados, exponiendo información de la infraestructura.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador podría interpretar archivos de forma incorrecta (MIME-type sniffing), facilitando la ejecución de código no deseado.
[MEDIUM] Referrer-Policy: No se controla qué información de navegación se envía a otros sitios web cuando el usuario hace clic en enlaces externos.
[MEDIUM] Permissions-Policy: El sitio no restringe el uso de APIs del navegador como la cámara o el micrófono, lo que aumenta el riesgo en caso de compromiso del sitio.
[MEDIUM] Cookies sin SameSite: Las cookies de sesión no cuentan con el atributo SameSite, lo que las hace vulnerables a ataques de Cross-Site Request Forgery (CSRF).
[LOW] Server header expuesto: El servidor revela la versión exacta Apache/2.4.58 (Ubuntu), lo que permite a posibles atacantes buscar vulnerabilidades específicas para ese software.
[LOW] Archivos robots.txt y sitemap.xml no encontrados: La ausencia de estos archivos dificulta la auditoría de indexación y puede reflejar una falta de mantenimiento preventivo.