EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://campusvirtualtrimestral.unah.edu.hn/my/	Checks	9 pruebas
Dominio	campusvirtualtrimestral.unah.edu.hn	Hallazgos	47 totales
Fecha	20 de mayo de 2026 a las 21:49	Problemas	8 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio campusvirtualtrimestral.unah.edu.hn arroja una puntuación de 80/100, lo que equivale a una calificación de grado B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, se emitió una advertencia y se registraron 2 fallos en configuraciones críticas. Si bien la infraestructura de cifrado y red es sólida, la ausencia de políticas de seguridad en las cabeceras HTTP y la configuración incompleta de cookies representan un riesgo. Se concluye que el sitio es funcionalmente seguro, pero vulnerable a ataques específicos de inyección de código y suplantación de peticiones.

Resumen de Riesgos

0	1	4	3	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 287 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 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	67	AVISO	MoodleSession: falta SameSite
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	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 287 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  287 dias restantes (expira: 2027-03-03T16:16:06.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-30T16:16:07.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx/1.28.0 — 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; preload
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://campusvirtualtrimestral.unah.edu.hn/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- 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

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 — 67/100

Estado: AVISO

MoodleSession: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: MoodleSession — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- 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

2 puerto(s) abierto(s), todos esperados

- 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)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — 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: Falta esta cabecera esencial que previene ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[MEDIUM] X-Content-Type-Options: La ausencia de esta cabecera permite el MIME-type sniffing, lo que puede llevar al navegador a ejecutar archivos con contenido inesperado.
[MEDIUM] Referrer-Policy: No existe una política configurada para controlar cuánta información de referencia se envía a otros sitios web al navegar.
[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de APIs del navegador, como la cámara, el micrófono o la geolocalización.
[MEDIUM] Cookie MoodleSession sin SameSite: Esta cookie de sesión carece del atributo SameSite, lo que expone a los usuarios a ataques de Cross-Site Request Forgery (CSRF).
[LOW] Server header expuesto: El servidor revela explícitamente el uso de nginx/1.28.0, información que un atacante puede usar para buscar exploits específicos.
[LOW] robots.txt no encontrado: El archivo de instrucciones para rastreadores no está presente, lo que dificulta la gestión de la indexación.
[LOW] sitemap.xml no encontrado: La ausencia de este archivo puede afectar la visibilidad y el rastreo organizado de la estructura del sitio.