

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://campus.uveg.edu.mx
Dominio campus.uveg.edu.mx
Fecha 25 de abril de 2026 a las 03:38

Checks 9 pruebas
Hallazgos 46 totales
Problemas 11 detectados

C

67/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre el dominio analizado arroja una puntuación de 67/100, lo que equivale a una nota de C. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron calificados como fallos críticos. Aunque la base de cifrado es sólida, se han detectado debilidades significativas en la configuración de cabeceras de seguridad y en la protección de las sesiones de usuario. Por lo tanto, se concluye que el sitio es actualmente vulnerable a ataques dirigidos contra los usuarios finales y de interceptación de datos de sesión.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 285 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	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 285 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
285 dias restantes (expira: 2027-02-03T23:59:00Z)
- INFO **Fecha de emision**
Emitido desde: 2026-01-05T00:00:00Z
- 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, X-Frame-Options, Strict-Transport-Security, Referrer-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
- **ALTO** **X-Frame-Options**
Falta — Protege contra clickjacking
- **ALTO** **Strict-Transport-Security**
Falta — Fuerza conexiones HTTPS (HSTS)
- **INFO** **X-Content-Type-Options**
Presente: nosniiff
- **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://campus.uveg.edu.mx:443/
- **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 — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- **INFO** **Cookies detectadas**
1 cookie(s) encontrada(s)
- **ALTO** **Cookie: PHPSESSID — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- **ALTO** **Cookie: PHPSESSID — Secure**
Falta flag Secure — Cookie se envia en conexiones HTTP
- **MEDIO** **Cookie: PHPSESSID — 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 (113 bytes)
- **INFO** **Reglas robots.txt**
1 Disallow, 3 Allow
- **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 autentificacion 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 permite la ejecución de scripts no autorizados, facilitando ataques de XSS e inyección de contenido.

[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking, permitiendo que un atacante cargue la web en marcos invisibles para engañar al usuario.

[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras, dejando la puerta abierta a ataques de degradación de protocolo (SSL Stripping).

[HIGH] Cookie PHPSESSID (Falta HttpOnly): Esta cookie de sesión es accesible mediante JavaScript, lo que permite a un atacante robar el identificador de sesión en caso de un XSS exitoso.

[HIGH] Cookie PHPSESSID (Falta Secure): El atributo Secure no está presente, lo que significa que la información de sesión podría transmitirse a través de conexiones HTTP no cifradas.

[MEDIUM] Cookie PHPSESSID (Falta SameSite): La carencia de esta directiva incrementa el riesgo de ataques de falsificación de petición en sitios cruzados (CSRF).

[MEDIUM] Referrer-Policy: No existe una política definida para controlar la información de procedencia enviada a sitios de terceros, comprometiendo la privacidad de los flujos de navegación.

[MEDIUM] Permissions-Policy: No se han restringido las APIs del navegador, permitiendo potencialmente que funciones como la cámara o el micrófono sean accedidas si existen otras vulnerabilidades.

[LOW] Server header expuesto: El servidor revela el uso de Apache en su cabecera de respuesta, proporcionando información técnica valiosa para que un atacante busque exploits específicos.

[LOW] sitemap.xml no encontrado: La falta de este archivo dificulta la auditoría estructurada y la indexación correcta de los recursos disponibles en el servidor.