

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://sigma.upla.edu.pe/academico/horario
Dominio sigma.upla.edu.pe
Fecha 23 de abril de 2026 a las 21:59

Checks 9 pruebas
Hallazgos 46 totales
Problemas 14 detectados

C

61/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 61/100, lo que equivale a una nota C. Durante la evaluación pasiva se ejecutaron 9 comprobaciones, de las cuales 6 resultaron satisfactorias y 3 presentaron fallos críticos relacionados con la configuración de red y cabeceras. Aunque el cifrado de datos es correcto, la ausencia de políticas de seguridad modernas y la falta de redirección forzosa a HTTPS comprometen la integridad de la plataforma. En conclusión, el sitio se considera vulnerable ante ataques de interceptación y manipulación de contenido debido a estas carencias técnicas.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 80 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	100	OK	No se encontraron cookies
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 80 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
80 dias restantes (expira: 2026-07-12T23:59:59.000Z)
- INFO **Fecha de emision**
Emitido desde: 2025-06-11T00:00:00.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
Server: Microsoft-IIS/10.0 — Revela tecnologia del servidor

- **BAJO** **X-Powered-By expuesto**
X-Powered-By: ASP.NET — Revela framework/lenguaje
- **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)
- **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 — 0/100

Estado: **FALLO**

No hay redireccion HTTP a HTTPS

- **ALTO** **HTTP !' HTTPS redireccion**
HTTP 404 — No dirige a HTTPS
- **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
- **INFO** **Tecnologias detectadas**
ASP.NET

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)
- **MEDIO** **Ruta /administrator/**
Panel de login accesible publicamente

- MEDIO** Ruta /user/login
Panel de login accesible publicamente
- INFO** Version CMS
No se detecta ninguna version expuesta

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 — 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 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, aumentando el riesgo de ataques XSS.

[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking que pueden engañar a los usuarios.

[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador obligue siempre el uso de conexiones cifradas, facilitando ataques de degradación.

[HIGH] Redirección HTTP a HTTPS: El sistema no redirige automáticamente el tráfico inseguro al protocolo seguro, dejando datos expuestos en tránsito.

[MEDIUM] X-Content-Type-Options: Su falta permite que el navegador intente adivinar el tipo de contenido, lo que puede derivar en la ejecución de archivos maliciosos.

[MEDIUM] Referrer-Policy: No se controla qué información de procedencia se envía a otros sitios al hacer clic en enlaces externos.

[MEDIUM] Permissions-Policy: No existen restricciones sobre el acceso a funciones del navegador como la ubicación o periféricos.

[MEDIUM] Paneles de login expuestos: Las rutas /administrator/ y /user/login son accesibles desde internet, facilitando intentos de acceso no autorizado.

[LOW] Server header expuesto: El servidor revela el uso de Microsoft-IIS/10.0, proporcionando información valiosa para atacantes que busquen exploits específicos.

[LOW] X-Powered-By expuesto: Se identifica públicamente el uso de ASP.NET como framework de desarrollo.

[LOW] Ausencia de robots.txt y sitemap.xml: El sitio carece de archivos de guía para buscadores, lo que afecta la gestión de indexación de rutas.