EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://campus.unap.edu.pe/login?ReturnUrl=%2Fconnect%2Fauthorize%2Fcallback%3Fclient_id%3Dlaurassia%26redirect_uri%3Dhttps%253A%252F%252Faulavirtual2.unap.edu.pe%252Fsignin-oidc%26response_type%3Dcode%26scope%3Dopenid%2520profile%2520roles%26code_challenge%3DAkYVjKAHOKbyomM0wQ7eTIJskJz2-DeCqGVT7przFrg%26code_challenge_method%3DS256%26response_mode%3Dform_post%26nonce%3D639156079864825743.ODY4YTU0ZWYtNjFkNy00ZmEwLWE2NWItM2EwMGQ1NDkzZGZmMmVkODcyNmMtNzRlYS00MGY1LTgzYTktYzVkZjEzMzAwYzFk%26state%	Checks	9 pruebas
Dominio	campus.unap.edu.pe	Hallazgos	49 totales
Fecha	28 de mayo de 2026 a las 23:34	Problemas	11 detectados

C

71/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado ha arrojado una puntuación de 71/100, lo que equivale a una nota de C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 presentaron fallos críticos. Aunque la base de cifrado es correcta, existen debilidades importantes en la configuración de las cabeceras de seguridad y el manejo de cookies. Por tanto, se concluye que el sitio es vulnerable ante ataques de inyección y posibles interceptaciones de datos de sesión.

Resumen de Riesgos

0	5	3	3	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 84 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	67	AVISO	.AspNetCore.Antiforgery.DvYER2SviNY: falta Secur...
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 84 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  84 dias restantes (expira: 2026-08-20T16:05:52.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-22T16:05:53.000Z
- 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: nginx/1.16.1 — 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://campus.unap.edu.pe/
- 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**
  Next.js

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

.AspNetCore.Antiforgery.DvYER2SviNY: falta Secure; .AspNetCore.Mvc.CookieTempDataProvider: falta Secure

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: .AspNetCore.Antiforgery.DvYER2SviNY — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: .AspNetCore.Antiforgery.DvYER2SviNY — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: .AspNetCore.Antiforgery.DvYER2SviNY — SameSite**
  SameSite=strict
- INFO **Cookie: .AspNetCore.Mvc.CookieTempDataProvider — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: .AspNetCore.Mvc.CookieTempDataProvider — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: .AspNetCore.Mvc.CookieTempDataProvider — SameSite**
  SameSite=lax

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: Su ausencia facilita ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] Strict-Transport-Security: La falta de esta directiva impide que el navegador fuerce conexiones HTTPS de forma automática.
[HIGH] Cookie .AspNetCore.Antiforgery sin flag Secure: El token de seguridad puede ser transmitido sobre conexiones no cifradas, exponiéndolo a interceptación.
[HIGH] Cookie .AspNetCore.Mvc.CookieTempDataProvider sin flag Secure: Los datos temporales de la sesión carecen de la protección necesaria para transmisiones exclusivas vía HTTPS.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite ataques de MIME-sniffing, donde el navegador interpreta archivos de forma incorrecta.
[MEDIUM] Referrer-Policy: No hay control sobre la información de origen que se envía a otros dominios, lo que podría filtrar rutas internas.
[MEDIUM] Permissions-Policy: No se restringe el acceso a funciones sensibles del navegador como la cámara o el micrófono.
[LOW] Server header expuesto: La cabecera revela la versión específica nginx/1.16.1, lo cual facilita la búsqueda de exploits conocidos.
[LOW] robots.txt no encontrado: La ausencia de este archivo indica una falta de configuración básica en la gestión del rastreo web.
[LOW] sitemap.xml no encontrado: La inexistencia de este mapa del sitio dificulta la auditoría de rutas y la indexación controlada.