EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.up.ac.pa	Checks	9 pruebas
Dominio	www.up.ac.pa	Hallazgos	54 totales
Fecha	25 de abril de 2026 a las 01:40	Problemas	18 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arrojó una puntuación de 65/100, lo que equivale a una nota de C. El análisis se basó en 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 2 generaron advertencias y 3 fueron calificados como fallos. Aunque el cifrado SSL es robusto, existen deficiencias críticas en las cabeceras de seguridad y en la protección de las cookies de sesión. Se detectaron múltiples recursos de contenido mixto que comprometen la integridad de la navegación. En su estado actual, el sitio se considera vulnerable ante ataques de interceptación y suplantación.

Resumen de Riesgos

0	4	8	6	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 269 dias
Cabeceras de Seguridad	30	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: Drupal
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	33	FALLO	cookiesession1: falta Secure; cookiesession1: fa...
Contenido Mixto	20	FALLO	11 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 269 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  269 dias restantes (expira: 2027-01-18T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-12-19T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 30/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache/2.4.58 (codeit) OpenSSL/3.0.12+quic PHP/7.4.33 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/7.4.33 — Revela framework/lenguaje
- 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)
- INFO **X-Content-Type-Options**
  Presente: nosniff, nosniff
- 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://www.up.ac.pa: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

CMS detectado: Drupal

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  Detectado via HTML body
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Drupal 9 (https://www.drupal.org)
- INFO **Tecnologias detectadas**
  Next.js, Astro, PHP/7.4.33

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 33/100

Estado: FALLO

cookiesession1: falta Secure; cookiesession1: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: cookiesession1 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: cookiesession1 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: cookiesession1 — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 20/100

Estado: FALLO

11 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://upmail.up.ac.pa/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://upintranet.up.ac.pa/Intranet/Logins.aspx
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.sibiup.up.ac.pa/
- MEDIO **href (link/stylesheet)**
  ...y 8 mas del mismo tipo

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1706 bytes)
- INFO **Reglas robots.txt**
  26 Disallow, 18 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- 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: Falta esta cabecera esencial, lo que deja el sitio vulnerable a ataques de inyección de contenido y XSS.
[HIGH] Strict-Transport-Security: La ausencia de HSTS impide que el navegador fuerce conexiones seguras, permitiendo posibles degradaciones a HTTP.
[HIGH] Cookie insegura (cookiesession1): El flag Secure no está configurado, permitiendo que la cookie se transmita por canales no cifrados.
[MEDIUM] Cookie sin atributo SameSite: La cookie cookiesession1 carece de protección contra ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto: Se identificaron 11 recursos cargados mediante HTTP en una página protegida por HTTPS, lo que debilita la seguridad global.
[MEDIUM] Referrer-Policy y Permissions-Policy: La ausencia de estas cabeceras expone información de navegación y no restringe el acceso a APIs sensibles del navegador.
[MEDIUM] Archivo informativo expuesto: El archivo /README.txt es accesible públicamente, lo que facilita a atacantes obtener detalles técnicos sobre la instalación de Drupal.
[LOW] Exposición de tecnología en cabeceras: El servidor revela versiones exactas de Apache, PHP y OpenSSL, facilitando la búsqueda de exploits específicos.
[LOW] Divulgación de rutas en robots.txt: Se referencian directorios como admin y config, exponiendo posibles puntos de entrada sensibles para el reconocimiento.