EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://mesadepartes.eesppindoamerica.edu.pe	Checks	9 pruebas
Dominio	mesadepartes.eesppindoamerica.edu.pe	Hallazgos	42 totales
Fecha	10 de agosto de 2026 a las 17:52	Problemas	9 detectados

B

77/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del dominio mesadepartes.eesppindoamerica.edu.pe ha resultado en una puntuación de 77/100 y una nota B. Se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 generó una advertencia y 2 fueron identificados como fallos técnicos. Aunque el sitio web cuenta con un cifrado de transporte robusto, carece de múltiples mecanismos de defensa en profundidad a nivel de cabeceras HTTP. Por lo tanto, el sitio se considera funcionalmente seguro en su comunicación, pero vulnerable a ataques específicos de manipulación del lado del cliente y secuestro de clics.

Resumen de Riesgos

0	3	3	3	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 78 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
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	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	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 78 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  78 dias restantes (expira: 2026-10-27T22:54:29.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-29T22:54:30.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: hcdn — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://mesadepartes.eesppindoamerica.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

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 — 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

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] X-Frame-Options: La cabecera está ausente, lo que permite que el sitio sea cargado en iframes y facilita ataques de clickjacking.
[HIGH] Strict-Transport-Security: La falta de configuración HSTS impide que el navegador fuerce conexiones seguras permanentemente, permitiendo posibles degradaciones de protocolo.
[MEDIUM] X-Content-Type-Options: El servidor no bloquea el sniffing de tipos MIME, lo que podría permitir la ejecución de archivos maliciosos disfrazados de contenido estático.
[MEDIUM] Referrer-Policy: No se ha definido una política de referencia, lo que puede provocar la fuga de información sensible de la URL a sitios de terceros.
[MEDIUM] Permissions-Policy: La falta de esta cabecera permite que el sitio acceda potencialmente a funciones del navegador como cámara o ubicación sin restricciones granulares.
[LOW] Server header expuesto: Se detectó la cabecera Server: hcdn, lo cual revela información técnica sobre la infraestructura que un atacante podría utilizar para ataques dirigidos.

[LOW] robots.txt: El archivo de instrucciones para rastreadores no fue encontrado (Error 404), dificultando la gestión de la indexación.
[LOW] sitemap.xml: El mapa del sitio no está disponible, lo que afecta la visibilidad estructurada de los contenidos de la web.