EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://iftc.edu.do	Checks	9 pruebas
Dominio	iftc.edu.do	Hallazgos	47 totales
Fecha	23 de abril de 2026 a las 11:20	Problemas	14 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de ciberseguridad realizado al sitio web ha arrojado una puntuacion de 61/100, lo que equivale a una nota de C. Durante la evaluacion se ejecutaron 9 checks pasivos, de los cuales 4 resultaron exitosos, 2 generaron advertencias y 2 fueron calificados como fallos, junto con un error por tiempo de espera en un modulo especifico. La infraestructura presenta debilidades importantes en la configuracion de cabeceras de seguridad y en la proteccion de las sesiones de usuario. Se concluye que el sitio es vulnerable a ataques de secuestro de sesion, clickjacking e inyeccion de contenido debido a la ausencia de politicas de seguridad fundamentales.

Resumen de Riesgos

0	6	5	3	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 49 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	CMS detectado: WordPress, PrestaShop
Seguridad de Cookies	0	FALLO	mphb_session: falta HttpOnly; mphb_session: falt...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 49 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  49 dias restantes (expira: 2026-06-11T20:20:00.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-13T20:20:01.000Z
- 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, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — 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)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- INFO **Permissions-Policy**
  Presente: private-state-token-redemption=(self "https://www.google.com" "https://www.gstat...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://iftc.edu.do/
- 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: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.8.5
- INFO **Tecnologias detectadas**
  Next.js, Astro

Seguridad de Cookies — 0/100

Estado: FALLO

mphb_session: falta HttpOnly; mphb_session: falta Secure; mphb_session: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: mphb_session — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: mphb_session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: mphb_session — 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (2006 bytes)
- INFO **Reglas robots.txt**
  11 Disallow, 2 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://iftc.edu.do/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: Falta la cabecera CSP, lo que permite la ejecucion de scripts no autorizados y ataques XSS.
[HIGH] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, por lo que el navegador no fuerza conexiones cifradas permanentemente.
[HIGH] Cookie: mphb_session (HttpOnly): La falta de este atributo permite que la cookie sea accesible mediante scripts, aumentando el riesgo de robo de sesion.

[HIGH] Cookie: mphb_session (Secure): La cookie carece del flag de seguridad, permitiendo su transmision a traves de canales HTTP no cifrados.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite a los navegadores realizar sniffing de tipos MIME, lo que puede derivar en ejecucion de codigo malicioso.
[MEDIUM] Referrer-Policy: No se controla la informacion de referencia enviada a sitios externos, comprometiendo la privacidad de la navegacion.
[MEDIUM] Cookie: mphb_session (SameSite): La ausencia de esta configuracion hace que el sitio sea susceptible a ataques de falsificacion de peticion en sitios cruzados (CSRF).
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detecto un puerto alternativo abierto que incrementa la superficie de exposicion ante posibles intrusiones.
[MEDIUM] Robots.txt (Bloqueo total): El archivo esta configurado para impedir la indexacion de todo el sitio, afectando su visibilidad y estructura.
[LOW] Server header expuesto: Se revela informacion tecnica sobre el uso de Cloudflare, ayudando a los atacantes en la fase de reconocimiento.
[LOW] Meta generator: La exposicion de la version de WordPress 6.8.5 permite identificar vulnerabilidades especificas asociadas a ese despliegue.
[LOW] Ruta sensible en robots.txt: Se mencionan rutas administrativas que dan pistas sobre la estructura interna del servidor a actores malintencionados.