EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://isfdyt20.edu.ar/	Checks	9 pruebas
Dominio	isfdyt20.edu.ar	Hallazgos	44 totales
Fecha	3 de abril de 2026 a las 19:02	Problemas	12 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al sitio web arroja una puntuación de 59/100, lo que equivale a una calificación de nota D. Se completaron un total de 9 checks pasivos, resultando en 5 aprobados, 2 advertencias y 2 fallos críticos relacionados con la configuración del servidor. El sitio presenta carencias fundamentales en la protección de la sesión del usuario y en el endurecimiento de las cabeceras de comunicación. Debido a la exposición de tecnologías obsoletas y la falta de cifrado forzado, se concluye que el sitio es actualmente vulnerable ante ataques de interceptación y explotación de software antiguo.

Resumen de Riesgos

0	5	4	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 59 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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 59 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  59 dias restantes (expira: 2026-06-01T13:46:02.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-03T13:46:03.000Z
- 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: Apache/2.4.25 (Win64) OpenSSL/1.0.2j PHP/5.6.30 — 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
- 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 200 — No redirige 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
- BAJO **Meta generator**
  Expone: Microsoft FrontPage 6.0

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (197 bytes)
- INFO **Reglas robots.txt**
  5 Disallow, 0 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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] Ausencia de Redirección HTTPS: El servidor no fuerza el tráfico cifrado, permitiendo conexiones HTTP inseguras que exponen los datos de los usuarios.
[HIGH] Falta de Content-Security-Policy: No existe una política para restringir el origen del contenido, facilitando ataques de inyección como Cross-Site Scripting (XSS).
[HIGH] Falta de X-Frame-Options: La carencia de esta cabecera permite que el sitio sea embebido en marcos externos, habilitando ataques de clickjacking.
[HIGH] Falta de Strict-Transport-Security: No se implementa HSTS, por lo que el navegador no puede garantizar que todas las conexiones futuras sean exclusivamente por HTTPS.

[MEDIUM] Falta de X-Content-Type-Options: La ausencia de protección contra MIME-sniffing permite que archivos cargados sean interpretados erróneamente por el navegador como scripts ejecutables.
[MEDIUM] Puerto 22 (SSH) abierto: La exposición pública de este puerto de administración remota incrementa significativamente la superficie de ataque para intentos de intrusión por fuerza bruta.
[MEDIUM] Falta de Referrer-Policy y Permissions-Policy: Se omite el control sobre la información de origen enviada en solicitudes y no se restringe el acceso a APIs sensibles del navegador.
[LOW] Tecnologías obsoletas expuestas: Se revela el uso de Apache/2.4.25 y PHP/5.6.30 a través de la cabecera Server, versiones que cuentan con vulnerabilidades conocidas públicamente.
[LOW] Uso de Microsoft FrontPage 6.0: La etiqueta meta generator indica el uso de una herramienta de desarrollo extremadamente antigua y fuera de soporte.
[LOW] Sitemap ausente: No se encontró el archivo sitemap.xml, lo que afecta la visibilidad controlada de la estructura del sitio por parte de motores de búsqueda.