EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://tubiflex.com.ar	Checks	9 pruebas
Dominio	tubiflex.com.ar	Hallazgos	49 totales
Fecha	22 de abril de 2026 a las 19:26	Problemas	13 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada sobre el dominio tubiflex.com.ar arroja una puntuacion de 65/100 con una calificacion final de nota C. Durante la evaluacion se ejecutaron 9 checks pasivos, de los cuales 5 resultaron correctos, 2 generaron advertencias y 2 fueron marcados como fallos criticos. El sitio web presenta deficiencias significativas en la configuracion de cabeceras de respuesta y en la gestion de seguridad de las cookies de sesion. En base a estos hallazgos, se concluye que el sitio es actualmente vulnerable a ataques de inyeccion, secuestro de sesion y falsificacion de solicitudes.

Resumen de Riesgos

0	5	5	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 56 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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	33	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Same...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 56 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  56 dias restantes (expira: 2026-06-17T15:42:23.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-19T15:42:24.000Z
- 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: LiteSpeed — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.2.16 — Revela framework/lenguaje
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://tubiflex.com.ar/
- 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, PHP/8.2.16

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 — 33/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: PHPSESSID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.stucchigroup.com/

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (506 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 4 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.tubiflex.com.ar/sitemap_index.xml
- 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 indispensable para prevenir ataques de Cross-Site Scripting (XSS) e inyeccion de contenido.
[HIGH] X-Frame-Options: La ausencia de esta cabecera deja el sitio vulnerable a ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que permite que el navegador acepte conexiones no cifradas.
[HIGH] Cookie PHPSESSID (HttpOnly): La cookie de sesion carece del atributo HttpOnly, permitiendo su acceso mediante scripts y facilitando el robo de sesion.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, aumentando el riesgo de ejecucion de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se controla la informacion de navegacion enviada a otros sitios a traves de los encabezados de referencia.
[MEDIUM] Permissions-Policy: No existen restricciones sobre las APIs del navegador como la camara, el microfono o la geolocalizacion.
[MEDIUM] Cookie PHPSESSID (SameSite): La ausencia del atributo SameSite hace que la sesion sea vulnerable a ataques de Cross-Site Request Forgery (CSRF).
[MEDIUM] Contenido Mixto: Se detecto un recurso externo (stucchigroup.com) cargado mediante HTTP, lo que compromete la integridad de la conexion cifrada.
[LOW] Server header expuesto: El servidor revela el uso de LiteSpeed, facilitando la busqueda de exploits especificos por parte de atacantes.
[LOW] X-Powered-By expuesto: Se revela la version exacta de PHP (8.2.16), informacion tecnica que no deberia ser publica.
[LOW] Ruta sensible en robots.txt: Se hace referencia a una ruta "admin" que podria indicar la ubicacion de paneles de gestion internos.