EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sso.secureserver.net/?realm=idp&path=%2Fpage%2Fsalvar_dados.php&app=host&auth_reason=1&plid=undefined	Checks	9 pruebas
Dominio	sso.secureserver.net	Hallazgos	62 totales
Fecha	23 de mayo de 2026 a las 02:03	Problemas	27 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre el dominio sso.secureserver.net ha arrojado una puntuación de 72/100, lo que corresponde a una calificación de grado C. El análisis se basó exclusivamente en 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron marcados como fallos críticos. A pesar de contar con un cifrado SSL robusto, se identificaron deficiencias severas en la configuración de cabeceras de seguridad y en la protección de cookies de sesión. Debido a estas vulnerabilidades en la gestión de la privacidad y la integridad de los datos, el sitio se considera vulnerable ante ataques de interceptación y secuestro de sesión.

Resumen de Riesgos

CRITICO	ALTO	MEDIO	BAJO	INFO
0	14	11	2	35

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 185 dias
Cabeceras de Seguridad	40	FALLO	Solo 2/6 presentes. Faltan: Strict-Transport-Sec...
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	0	FALLO	fb_sessiontraffic: falta HttpOnly; fb_sessiontra...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 185 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  185 dias restantes (expira: 2026-11-24T00:07:48.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-10-23T00:07:48.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 40/100

Estado: FALLO

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

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Express — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: frame-ancestors 'none'
- INFO **X-Frame-Options**
  Presente: deny
- 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://sso.secureserver.net/
- 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**
  React, Next.js, Express

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- 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 — 0/100

Estado: FALLO

fb_sessiontraffic: falta HttpOnly; fb_sessiontraffic: falta Secure; fb_sessiontraffic: falta SameSite; pathway: falta HttpOnly; pathway: falta Secure; pathway: falta SameSite; visitor: falta HttpOnly; visitor: falta Secure; visitor: falta SameSite; _policy: falta HttpOnly; _policy: falta Secure; _policy: falta SameSite; market: falta HttpOnly; market: falta Secure; market: falta SameSite; currency: falta HttpOnly; currency: falta Secure; currency: falta SameSite

- INFO **Cookies detectadas**
  6 cookie(s) encontrada(s)
- ALTO **Cookie: fb_sessiontraffic — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: fb_sessiontraffic — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: fb_sessiontraffic — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: pathway — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: pathway — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: pathway — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: visitor — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: visitor — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: visitor — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: _policy — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: _policy — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: _policy — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: market — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: market — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: market — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: currency — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: currency — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: currency — 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (127 bytes)

- INFO **Reglas robots.txt**
  6 Disallow, 0 Allow
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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] Falta de Strict-Transport-Security (HSTS): La ausencia de esta cabecera permite que las conexiones puedan ser degradadas de HTTPS a HTTP, facilitando ataques de hombre en el medio.
[HIGH] Cookies de sesión sin flag HttpOnly: Cookies como fb_sessiontraffic, pathway y visitor son accesibles mediante scripts, lo que permite el robo de identidad a través de ataques XSS.
[HIGH] Cookies de sesión sin flag Secure: Varias cookies se envían a través de conexiones no cifradas, exponiendo datos sensibles en redes no seguras.
[MEDIUM] Ausencia de cabeceras de protección: Faltan X-Content-Type-Options, Referrer-Policy y Permissions-Policy, lo que deja al navegador sin instrucciones para mitigar ataques de sniffing o fugas de información.
[MEDIUM] Cookies sin atributo SameSite: La falta de esta configuración en todas las cookies detectadas incrementa el riesgo de ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Archivos técnicos expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, lo que podría revelar detalles internos sobre la infraestructura o versiones del software.
[LOW] Exposición de tecnología en cabeceras: Se detectó el uso de Envoy y el framework Express en las cabeceras Server y X-Powered-By, proporcionando información valiosa para atacantes.