EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://uptaivirtualsarec.com/saeyce	Checks	9 pruebas
Dominio	uptaivirtualsarec.com	Hallazgos	44 totales
Fecha	18 de julio de 2026 a las 15:57	Problemas	14 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio uptaivirtualsarec.com/saeyce ha arrojado una puntuación de 57/100, lo que resulta en una calificación de grado D. Se ejecutaron un total de 9 controles pasivos, obteniendo 5 resultados satisfactorios, 1 advertencia y 3 fallos críticos en la configuración del servidor. El análisis revela una exposición peligrosa de servicios de infraestructura y una ausencia total de políticas de seguridad en las cabeceras HTTP. Debido a la apertura de puertos de bases de datos y la falta de cifrado forzado, se concluye que el sitio es actualmente vulnerable y presenta un riesgo significativo para la privacidad de los datos.

Resumen de Riesgos

1	6	3	4	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 44 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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 44 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  44 dias restantes (expira: 2026-08-31T04:02:56.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-02T04:02:57.000Z
- 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/5.6.40 — 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 — 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
- INFO **Tecnologias detectadas**
  PHP/5.6.40

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 — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL) abierto: La base de datos está expuesta directamente a internet, lo que permite ataques de fuerza bruta o explotación de vulnerabilidades del motor de datos.
[HIGH] Puerto 21 (FTP) abierto: Este servicio transmite información y credenciales sin cifrado, facilitando la interceptación de datos mediante ataques de hombre en el medio.

[HIGH] Falta de redirección HTTP a HTTPS: El servidor no fuerza el uso de conexiones seguras, permitiendo que la navegación ocurra a través de canales no cifrados.
[HIGH] Ausencia de HSTS (Strict-Transport-Security): El sitio no instruye al navegador para usar exclusivamente HTTPS, dejando la conexión vulnerable a ataques de degradación de seguridad.
[HIGH] Content-Security-Policy (CSP) faltante: No existe una política que restrinja el origen del contenido, lo que facilita ataques de inyección de scripts (XSS).
[HIGH] X-Frame-Options faltante: La ausencia de esta cabecera hace que el sitio sea susceptible a ataques de clickjacking para engañar a los usuarios.
[MEDIUM] X-Content-Type-Options faltante: El servidor no previene el sniffing de tipos MIME, permitiendo que archivos maliciosos sean interpretados como scripts ejecutables.
[MEDIUM] Referrer-Policy faltante: No se controla la información de procedencia enviada a sitios externos, lo que puede filtrar URLs privadas o tokens de sesión.
[MEDIUM] Permissions-Policy faltante: El sitio no restringe el acceso de las APIs del navegador a funciones sensibles como la cámara, el micrófono o la ubicación.
[LOW] Cabecera Server expuesta (LiteSpeed): Se revela la tecnología exacta del servidor, facilitando a los atacantes la búsqueda de exploits específicos para esa plataforma.
[LOW] Cabecera X-Powered-By expuesta (PHP/5.6.40): El uso de una versión de PHP obsoleta y su exposición pública simplifica la planificación de un ataque dirigido.
[LOW] Ausencia de archivos robots.txt y sitemap.xml: La falta de estos archivos indica una gestión de rastreo deficiente y puede exponer rutas que no deberían ser indexadas.