INFORME TÉCNICO DE ESCANEO DE VULNERABILIDADES - ASHIRA SOFTWARE

Resumen Ejecutivo

Se ha realizado un análisis de seguridad integral del sitio web ASHIRA SOFTWARE (`https://ashira.click/`), que maneja datos sensibles de salud. Los resultados, obtenidos mediante herramientas especializadas (OWASP ZAP y Nikto Security Scanner), indican una calificación de seguridad de **66/100 (Grado C)**.

Se identificaron **3 vulnerabilidades críticas** de nivel medio que requieren atención inmediata, principalmente relacionadas con la configuración de cabeceras HTTP y DNS, lo cual pone en riesgo la integridad de los datos de pacientes y el cumplimiento normativo (**HIPAA/GDPR**). La implementación de las recomendaciones detalladas en este informe es esencial para mitigar riesgos como el Cross-Site Scripting (XSS), el robo de sesiones y la falsificación de correos electrónicos.

Hallazgos por Nivel de Riesgo

Riesgo	Cantidad	Descripción	Prioridad
ALTO	0	Sin vulnerabilidades críticas inmediatas.	
MEDIO	3	Errores de configuración de seguridad críticos (CORS, CSP, Clickjacking).	**ALTA**
BAJO	1	Ausencia de cabecera `X-Content-Type-Options`.	MEDIA

Riesgo	Cantidad	Descripción	Prioridad
INFORMATIVO	12	Hallazgos menores (Subdominios expuestos, Cache inadecuada, DNS).	BAJA

---

1. Vulnerabilidades Críticas (Riesgo Medio)

Estas vulnerabilidades deben ser abordadas en la **Semana 1** del plan de acción.

1.1. Configuración Incorrecta de CORS (Cross-Origin Resource Sharing)

Nivel	Impacto
⚠ MEDIO	Permite solicitudes de lectura de recursos no autenticados desde dominios arbitrarios, facilitando el acceso a datos sensibles por parte de terceros.

Hallazgo: La cabecera `Access-Control-Allow-Origin: *` está presente.
Recomendación: Restringir esta configuración para solo permitir una lista blanca de dominios específicos (e.g., `https://ashira.click`, `https://app.ashira.click`).

1.2. Falta de Content Security Policy (CSP)

Nivel	Impacto
⚠ MEDIO	**Ausencia total** de la cabecera `Content-Security-Policy`. Es la defensa principal contra ataques de Cross-Site Scripting (XSS) y la inyección de código.

Hallazgo: El servidor no envía la cabecera `Content-Security-Policy`.
Recomendación: Implementar una política estricta que defina las fuentes de contenido permitidas (`default-src 'self'`).

1.3. Falta de Protección Anti-Clickjacking

Nivel	Impacto
⚠ MEDIO	La ausencia de protección expone a los usuarios a ser engañados para realizar acciones no deseadas a través de iframes maliciosos.

Hallazgo: Ausencia de las cabeceras `X-Frame-Options` y la directiva `frame-ancestors` en CSP.
Recomendación: Implementar `X-Frame-Options: DENY` o `SAMEORIGIN` y la directiva `frame-ancestors 'none';` en la CSP.

---

2. Vulnerabilidades Moderadas e Informativas

2.1. Ausencia de Registros SPF y DMARC (Vulnerabilidad BAJA)

Nivel	Impacto
🔵 BAJO	El dominio es vulnerable a email spoofing (falsificación de correos electrónicos), lo cual es crítico para una plataforma de salud.

Recomendaciones:

1. **Registro SPF:** Añadir un registro TXT que defina los servidores de correo autorizados, como: `ashira.click. IN TXT "v=spf1 include:_spf.google.com include:spf.protection.outlook.com -all"`
2. **Registro DMARC:** Implementar un registro TXT que indique la política de manejo de correos no autenticados, como: `_dmarc.ashira.click. IN TXT "v=DMARC1; p=reject; rua=mailto:security@ashira.click; ruf=mailto:security@ashira.click; fo=1"`

2.2. Superficie de Ataque Amplia (Hallazgo INFORMATIVO)

Se detectaron **96 subdominios** activos, incluyendo: `admin.ashira.click`, `api.ashira.click`, `app.ashira.click`, `auth.ashira.click`,

`dashboard.ashira.click`, `billing.ashira.click`, `chat.ashira.click`, y `cdn.ashira.click`.

Recomendaciones:

- Auditar inventario de subdominios para verificar su estado y aplicar políticas de seguridad específicas.
- Implementar Autenticación de Dos Factores (2FA) en todos los subdominios administrativos y un WAF (Web Application Firewall).

2.3. Control de Caché Inadecuado (Hallazgo INFORMATIVO)

Nivel	Impacto
ℹ️ INFORMATIVO	La configuración actual permite el almacenamiento en caché de contenido potencialmente sensible (`Cache-Control: public`) en el lado del cliente.

Recomendación: Configurar directivas de `Cache-Control` estrictas (`no-cache, no-store, must-revalidate, private`) en todas las rutas que manejen datos de pacientes o información de sesión (e.g., `/login`, `/dashboard`, `/api`).

---

3. Plan de Acción Prioritario

El siguiente plan de acción define las tareas necesarias para alcanzar el objetivo de seguridad de 90+/100.

Semana 1: Configuración Crítica

Esta semana se centra en la implementación de las 3 vulnerabilidades de riesgo medio.

Tarea	Responsable	Fecha Límite
Implementar cabeceras CSP, X-Frame-Options y X-Content-Type-Options	Person	Date
Configurar CORS restrictivo a lista blanca de dominios	Person	Date

Tarea	Responsable	Fecha Límite
Configurar registros DNS SPF y DMARC	Person	Date
Implementar HSTS con `includeSubDomains`	Person	Date

Semana 2: Protección de Datos y Ecosistema

Tarea	Responsable	Estado
Implementar políticas de caché estrictas para contenido sensible	Person	
Auditar, proteger y/o eliminar subdominios críticos	Person	
Configurar WAF en el entorno de despliegue (Vercel/Cloudflare)	Person	

4. Conclusión

El estado actual de seguridad del sitio de ASHIRA SOFTWARE es mejorable, con una calificación inicial de **66/100**. La rápida implementación de las cabeceras de seguridad y la configuración de DNS son los pasos más críticos y generarán el mayor retorno en la mitigación de riesgos.

La corrección de estas vulnerabilidades elevará la postura de seguridad, protegiendo la confidencialidad e integridad de la información médica de los pacientes y avanzando hacia el cumplimiento de regulaciones como HIPAA y GDPR.

Objetivo Post-Implementación: 90+/100.