Informe de Análisis de Seguridad - Aplicación Médica

Fecha de análisis: 2025-12-04

- OWASP Application Security Verification Standard (ASVS) Versión 4.0.3

- OWASP Web Security Testing Guide (WSTG)

Nota: Este informe ha sido generado automáticamente mediante análisis de código e integración con DefectDojo.

1. Descripción Breve de la Aplicación Analizada

1.1. Propósito y Funcionalidad

La aplicación es una herramienta web monousuario diseñada para el registro personal de peso, talla y cálculo del Índice de Masa Corporal (IMC). Su objetivo principal es permitir a un único usuario realizar un seguimiento de su peso corporal y obtener información sobre su estado nutricional mediante el cálculo automático del IMC.

1.2. Características Principales

• Registro de datos personales: Nombre, apellidos, fecha de nacimiento y talla (en metros)
• Registro de peso: Permite registrar el peso actual con fecha y hora automáticas
• Cálculo automático de IMC: Calcula y muestra el Índice de Masa Corporal basado en el último peso registrado
• Estadísticas históricas: Muestra número de pesajes, peso máximo y peso mínimo registrados
• Sincronización bidireccional: Entre frontend (localStorage) y backend (memoria)
• Modo offline: Funciona sin conexión al servidor utilizando almacenamiento local

1.3. Arquitectura Técnica

• Backend: Flask (Python) con API REST
• Frontend: JavaScript vanilla con almacenamiento en localStorage
• Almacenamiento: Memoria en backend + localStorage en frontend
• Tests: 86 tests backend (pytest) + ~66 tests frontend (Jest)
• Gestión de vulnerabilidades: DefectDojo integrado para seguimiento de debilidades de seguridad

1.4. Análisis de Datos que Maneja la Aplicación

La aplicación maneja diferentes tipos de datos que requieren diferentes niveles de protección:

1.4.1. Datos Sensibles (Personales de Salud)

• Peso corporal (kg): Dato biométrico personal
• Talla/Altura (m): Dato biométrico personal
• Fecha de nacimiento: Permite inferir edad y otros datos demográficos
• Nombre completo: Identificador personal
• Apellidos: Identificador personal
Clasificación según RGPD: Estos datos están categorizados como datos personales sensibles según el Reglamento General de Protección de Datos, ya que los datos de salud (peso, altura, IMC) están incluidos en la categoría de datos especiales.

Almacenamiento actual:

- Frontend: localStorage del navegador (cliente)

- Backend: Memoria (volátil, se pierde al reiniciar)

2. Análisis de Seguridad Realizado

2.1. Metodología

El análisis de seguridad se ha realizado mediante:

- Integración con DefectDojo: Obtención de benchmarks ASVS y findings reales

- Análisis estático de código: Revisión del código fuente Python y JavaScript

- Verificación de cumplimiento ASVS 4.0.3: Comparación con requisitos del estándar

- Mapeo de findings: Relación de vulnerabilidades con requisitos ASVS

- Análisis de arquitectura: Revisión de la estructura y diseño de la aplicación

2.2. Herramientas Utilizadas

• DefectDojo: Benchmarks ASVS y gestión de findings
• Análisis automático de código fuente
• Verificación de patrones de seguridad
• Comparación con estándares OWASP ASVS 4.0.3

3. Debilidades de Seguridad Identificadas

3.1. Resumen

El análisis automático ha identificado áreas de mejora en la aplicación. Las debilidades principales están relacionadas con:

- Validación de tipos numéricos (NaN/Infinity)

- Configuración de CORS para producción

- Mejora del logging de errores

4. Nivel ASVS Seleccionado, con Justificación

4.1. OWASP Application Security Verification Standard (ASVS)

Versión utilizada en este informe: ASVS 4.0.3 (versión estable, lanzada el 28 de octubre de 2021)

Fuente oficial: OWASP ASVS v4.0.3 en GitHub

El OWASP Application Security Verification Standard (ASVS) versión 4.0.3 es un estándar de seguridad para aplicaciones web que define tres niveles de verificación. Esta versión se centra en corregir errores ortográficos y clarificar requisitos sin introducir cambios significativos ni romper compatibilidad con versiones anteriores.

Estructura de categorías ASVS 4.0.3: 14 categorías de verificación (V1-V14):

- V1: Architecture, Design and Threat Modeling

- V2: Authentication

- V3: Session Management

- V4: Access Control

- V5: Validation, Sanitization and Encoding

- V6: Stored Cryptographically Sensitive Data
- V7: Error Handling and Logging
- V8: Data Protection
- V9: Communications
- V10: Malicious Code
- V11: Business Logic
- V12: Files and Resources
- V13: API
- V14: Configuration

4.2. Nivel Seleccionado: NIVEL 2 (ESTÁNDAR)

4.3. Justificación de la Selección

La aplicación maneja datos de salud personales (peso, altura, fecha de nacimiento), aunque no sean datos médicos críticos ni información de identificación sensible. Según el Reglamento General de Protección de Datos (RGPD), los datos de salud están categorizados como datos personales sensibles, lo que requiere un nivel de protección superior al básico.

4.4. Enumeración de Requerimientos ASVS Nivel 2

Basado en el análisis automático realizado, se enumeran TODOS los requerimientos ASVS Nivel 2 del estándar ASVS 4.0.3. El estándar ASVS 4.0.3 define 14 categorías de verificación (V1-V14) con sus respectivos subrequisitos. Se detallan todos los requisitos manteniendo la estructura exacta del estándar:

V1: Arquitectura, Diseño y Modelado de Amenazas

V1.1.1

Descripción: Verifique el uso de un ciclo de vida de desarrollo de software seguro que aborde la seguridad en todas las etapas del desarrollo. (C1)

Estado: PARCIAL

Explicación: El requisito V1.1.1 se cumple parcialmente. Se requiere revisión adicional.

V1.1.2

Descripción: Verifique el uso del modelado de amenazas para cada cambio de diseño o planificación de sprint para identificar amenazas, planificar contramedidas, facilitar respuestas de riesgo adecuadas y guiar las pruebas de seguridad.

Estado: PARCIAL

Explicación: El requisito V1.1.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-1053

V1.1.3

Descripción: Verifique que todas las historias y características de usuario contienen restricciones de seguridad funcionales, como por ejemplo: "Como usuario, debería poder ver y editar mi perfil. No debería ser capaz de ver o editar el perfil de nadie más"

Estado: PARCIAL

Explicación: El requisito V1.1.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-1110

V1.1.4

Descripción: Verifique la documentación y la justificación de todos los límites de confianza, componentes y flujos de datos significativos de la aplicación.

Estado: PARCIAL

Explicación: El requisito V1.1.4 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-1059

V1.1.5

Descripción: Verifique la definición y el análisis de seguridad de la arquitectura de alto nivel de la aplicación y todos los servicios remotos conectados. (C1)

Estado: PARCIAL

Explicación: El requisito V1.1.5 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-1059

V1.1.6

Descripción: Verifique la implementación de controles de seguridad centralizados, simples (economía del diseño), comprobados, seguros y reutilizables para evitar controles duplicados, faltantes, ineficaces o inseguros. (C10)

Estado: PARCIAL

Explicación: El requisito V1.1.6 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-637

V1.1.7

Descripción: Verifique la disponibilidad de una lista de comprobación de codificación segura, requisitos de seguridad, directriz o directiva para todos los desarrolladores y evaluadores.

Estado: PARCIAL

Explicación: El requisito V1.1.7 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-637

V1.2.1

Descripción: Verifique el uso de cuentas de sistema operativo únicas o especiales con privilegios bajos para todos los componentes, servicios y servidores de la aplicación. (C3)

Estado: CUMPLE

Explicación: El requisito V1.2.1 se cumple según el análisis realizado.

CWE relacionado: CWE-250

V1.2.2

Descripción: Verifique que las comunicaciones entre los componentes de la aplicación, incluidas las API, el middleware y las capas de datos, se autentican. Los componentes deben tener los mínimos privilegios necesarios. (C3)

Estado: CUMPLE

Explicación: El requisito V1.2.2 se cumple según el análisis realizado.

CWE relacionado: CWE-306

V1.2.3

Descripción: Verifique que la aplicación utiliza un único mecanismo de autenticación comprobado que se sabe que es seguro, se puede ampliar para incluir una autenticación segura y tiene suficiente logging y supervisión para detectar abuso de cuenta o brechas.

Estado: CUMPLE

Explicación: El requisito V1.2.3 se cumple según el análisis realizado.

CWE relacionado: CWE-306

V1.2.4

Descripción: Verifique que todas las vías de autenticación y las API de administración de identidades implementan una fortaleza coherente del control de seguridad de autenticación, de modo que no haya alternativas más débiles por el riesgo de la aplicación.

Estado: CUMPLE

Explicación: El requisito V1.2.4 se cumple según el análisis realizado.

CWE relacionado: CWE-306

V1.4.1

Descripción: Verifique que los puntos de cumplimiento de confianza, tales como puertas de enlace de control de acceso, servidores y funciones serverless, exijan controles de acceso. Nunca aplique controles de acceso en el cliente.

Estado: PARCIAL

Explicación: El requisito V1.4.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-602

V1.4.4

Descripción: Verifique que la aplicación utilice un mecanismo de control de acceso único y bien comprobado para acceder a datos y recursos protegidos. Todas las solicitudes deben pasar por este único mecanismo para evitar copiar y pegar o rutas alternativas inseguras. (C7)

Estado: PARCIAL

Explicación: El requisito V1.4.4 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-284

V1.4.5

Descripción: Verifique que se utiliza el control de acceso basado en atributos o entidades mediante el cual el código comprueba la autorización del usuario para un elemento de característica o datos en lugar de solo su rol. Los permisos deben asignarse mediante roles. (C7)

Estado: PARCIAL

Explicación: El requisito V1.4.5 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-275

V1.5.1

Descripción: Verifique que los requisitos de entrada y salida definan claramente cómo manejar y procesar datos en función del tipo, contenido y las leyes, regulaciones y otras leyes aplicables, reglamentos y otras normas de cumplimiento de políticas.

Estado: PARCIAL

Explicación: El requisito V1.5.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-1029

V1.5.2

Descripción: Verifique que no se usa serialización al comunicarse con clientes que no son de confianza. Si esto no es posible, asegúrese de que se apliquen controles de integridad adecuados (y posiblemente cifrado si se envían datos confidenciales) para evitar ataques de deserialización, incluida la inyección de objetos.

Estado: PARCIAL

Explicación: El requisito V1.5.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-502

V1.5.3

Descripción: Verifique que la validación de datos de entrada (input) se aplica en una capa de servicio de confianza. (C5)

Estado: PARCIAL

Explicación: El requisito V1.5.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-602

V1.5.4

Descripción: Verifique que la codificación de salida (output encode) se produce cerca o en el intérprete para el que está destinada. (C4)

Estado: PARCIAL

Explicación: El requisito V1.5.4 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-116

V1.6.1

Descripción: Verifique que existe una política explícita para la administración de claves criptográficas y que un ciclo de vida de clave criptográfica sigue un estándar de administración de claves como NIST SP 800-57.

Estado: PARCIAL

Explicación: El requisito V1.6.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-320

V1.6.2

Descripción: Verifique que los consumidores de servicios criptográficos protegen el material clave y otros secretos mediante el uso de almacenes de claves o alternativas basadas en API.

Estado: PARCIAL

Explicación: El requisito V1.6.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-320

V1.6.3

Descripción: Verifique que todas las claves y contraseñas son reemplazables y forman parte de un proceso bien definido para volver a cifrar los datos confidenciales.

Estado: PARCIAL

Explicación: El requisito V1.6.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-320

V1.6.4

Descripción: Verifique que la arquitectura trata los secretos del lado cliente (como claves simétricas, contraseñas o tokens de API) como inseguros y nunca los usa para proteger o acceder a datos confidenciales.

Estado: PARCIAL

Explicación: El requisito V1.6.4 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-320

V1.7.1

Descripción: Verifique que se utilice un formato común y un enfoque de logging en todo el sistema. (C9)

Estado: PARCIAL

Explicación: El requisito V1.7.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-1009

V1.7.2

Descripción: Verifique que los registros de log se transmitan de forma segura a un sistema preferentemente remoto para análisis, detección, alertas y escalamiento. (C9)

Estado: PARCIAL

Explicación: El requisito V1.7.2 se cumple parcialmente. Se requiere revisión adicional.

V1.8.1

Descripción: Verifique que todos los datos confidenciales se identifiquen y clasifiquen en niveles de protección.

Estado: PARCIAL

Explicación: El requisito V1.8.1 se cumple parcialmente. Se requiere revisión adicional.

V1.8.2

Descripción: Verifique que todos los niveles de protección tienen un conjunto asociado de requisitos de protección, como los requisitos de cifrado, los requisitos de integridad, la retención, la privacidad y otros requisitos de confidencialidad, y que estos se aplican en la arquitectura.

Estado: PARCIAL

Explicación: El requisito V1.8.2 se cumple parcialmente. Se requiere revisión adicional.

V1.9.1

Descripción: Verifique que la aplicación cifra las comunicaciones entre componentes, especialmente cuando estos componentes se encuentran en contenedores, sistemas, sitios o proveedores de nube diferentes. (C3)

Estado: PARCIAL

Explicación: El requisito V1.9.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-319

V1.9.2

Descripción: Verifique que los componentes de la aplicación verifiquen la autenticidad de cada lado en un vínculo de comunicación para evitar ataques de "persona en el medio". Por ejemplo, los componentes de la aplicación deben validar certificados y cadenas TLS.

Estado: PARCIAL

Explicación: El requisito V1.9.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-295

V1.10.1

Descripción: Verifique que un sistema de control de código fuente está en uso, con procedimientos para garantizar que los check-ins están respaldados tickets de issues o solicitudes de cambio. El sistema de control de código fuente debe tener control de acceso y usuarios identificables para permitir la trazabilidad de cualquier cambio.

Estado: PARCIAL

Explicación: El requisito V1.10.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-284

V1.11.1

Descripción: Verifique la definición y documentación de todos los componentes de la aplicación en términos de las funciones de negocio o de seguridad que proporcionan.

Estado: PARCIAL

Explicación: El requisito V1.11.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-1059

V1.11.2

Descripción: Verifique que todos los flujos de lógica de negocio de alto valor, incluida la autenticación, la administración de sesiones y el control de acceso, no compartan estados no sincronizados.

Estado: PARCIAL

Explicación: El requisito V1.11.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-362

V1.12.2

Descripción: Verifique que los archivos subidos por el usuario, -si es necesario que se muestren o descarguen desde la aplicación-, se hace mediante descargas de secuencias de octetos o desde un dominio no relacionado, como un almacenamiento de archivos en la nube. Implemente una directiva de seguridad de contenido (CSP) adecuada para reducir el riesgo de vectores XSS u otros ataques desde el archivo cargado.

Estado: PARCIAL

Explicación: El requisito V1.12.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-646

V1.14.1

Descripción: Verifique la segregación de componentes de diferentes niveles de confianza a través de controles de seguridad bien definidos, reglas de corta fuego, pasarelas de API, proxies reversos, grupos de seguridad basados en nube, o mecanismos similares.

Estado: PARCIAL

Explicación: El requisito V1.14.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-923

V1.14.2

Descripción: Verifique que las firmas binarias, las conexiones de confianza y los puntos de conexión verificados se usan para el despliegue de archivos binarios a dispositivos remotos.

Estado: PARCIAL

Explicación: El requisito V1.14.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-494

V1.14.3

Descripción: Verifique que el canal de compilación advierte de componentes obsoletos o inseguros y realiza las acciones adecuadas.

Estado: PARCIAL

Explicación: El requisito V1.14.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-1104

V1.14.4

Descripción: Verifique que el canal de compilación contiene un paso para compilar y comprobar automáticamente el despliegue seguro de la aplicación, especialmente si la infraestructura de la aplicación está definida por software, como los scripts de compilación del entorno en la nube.

Estado: PARCIAL

Explicación: El requisito V1.14.4 se cumple parcialmente. Se requiere revisión adicional.

V1.14.5

Descripción: Verifique que los despliegues de aplicaciones sean en sandbox, contenedores y/o aislados a nivel de red para retrasar e impedir que los atacantes vulneren otras aplicaciones, especialmente cuando realizan acciones sensibles o peligrosas, como la deserialización. (C5)

Estado: PARCIAL

Explicación: El requisito V1.14.5 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-265

V1.14.6

Descripción: Verifique que la aplicación no utiliza tecnologías del lado cliente no compatibles, inseguras o en desuso, como NSAPI plugins, Flash, Shockwave, ActiveX, Silverlight, NACL o client-side java applets.

Estado: PARCIAL

Explicación: El requisito V1.14.6 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-477

Estado de cumplimiento: PARCIAL

Explicación detallada:

V1.1: Falta documentación completa de arquitectura

V2: Autenticación

Estado general: NO APLICABLE

Justificación: Aplicación monousuario sin autenticación compleja

V2.1.1

Descripción: Verifique que las contraseñas del usuarios tienen al menos 12 caracteres de longitud (después de combinar varios espacios). (C6)

Estado: NO APLICABLE

Explicación: El requisito V2.1.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-521

V2.1.2

Descripción: Verifique que se permitan contraseñas de al menos 64 caracteres y que se denieguen contraseñas de más de 128 caracteres. (C6)

Estado: NO APLICABLE

Explicación: El requisito V2.1.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-521

V2.1.3

Descripción: Verifique que no se realiza el truncamiento de contraseña. Sin embargo, varios espacios consecutivos pueden ser reemplazados por un solo espacio. (C6)

Estado: NO APLICABLE

Explicación: El requisito V2.1.3 no es aplicable para esta aplicación.

CWE relacionado: CWE-521

V2.1.4

Descripción: Verifique que cualquier carácter Unicode imprimible, incluidos los caracteres neutros del idioma, como espacios y Emojis esté permitido en las contraseñas.

Estado: NO APLICABLE

Explicación: El requisito V2.1.4 no es aplicable para esta aplicación.

CWE relacionado: CWE-521

V2.1.5

Descripción: Verifique que los usuarios pueden cambiar su contraseña.

Estado: NO APLICABLE

Explicación: El requisito V2.1.5 no es aplicable para esta aplicación.

CWE relacionado: CWE-620

V2.1.6

Descripción: Verifique que la funcionalidad de cambio de contraseña requiere la contraseña actual y nueva del usuario.

Estado: NO APLICABLE

Explicación: El requisito V2.1.6 no es aplicable para esta aplicación.

CWE relacionado: CWE-620

V2.1.7

Descripción: Verifique que las contraseñas enviadas durante el registro de la cuenta, el inicio de sesión y el cambio de contraseña se comprueban localmente contra un conjunto de contraseñas filtradas (como las 1,000 o 10,000 contraseñas más comunes que coinciden con la directiva de contraseñas del sistema) o mediante una API externa. Si se utiliza una API, una prueba de zero knowledge u otro mecanismo, asegúrese que la contraseña en texto plano no se envía ni se utiliza para verificar el estado de filtración de la contraseña. Si la contraseña esta filtrada, la aplicación debe exigir al usuario que establezca una nueva contraseña no filtrada. (C6)

Estado: NO APLICABLE

Explicación: El requisito V2.1.7 no es aplicable para esta aplicación.

CWE relacionado: CWE-521

V2.1.8

Descripción: Verifique que se proporciona un medidor de fortaleza de la contraseña para ayudar a los usuarios a establecer una contraseña más segura.

Estado: NO APLICABLE

Explicación: El requisito V2.1.8 no es aplicable para esta aplicación.

CWE relacionado: CWE-521

V2.1.9

Descripción: Verifique que no hay reglas de composición de contraseñas que limiten el tipo de caracteres permitidos. No debe haber ningún requisito para mayúsculas o minúsculas o números o caracteres especiales. (C6)

Estado: NO APLICABLE

Explicación: El requisito V2.1.9 no es aplicable para esta aplicación.

CWE relacionado: CWE-521

V2.1.10

Descripción: Verifique que no haya rotación periódica de credenciales o solicitud del historial de contraseñas.

Estado: NO APLICABLE

Explicación: El requisito V2.1.10 no es aplicable para esta aplicación.

CWE relacionado: CWE-263

V2.1.11

Descripción: Verifique que se permite la funcionalidad "pegar", las aplicaciones auxiliares de contraseñas del browser y los administradores externos de contraseñas.

Estado: NO APLICABLE

Explicación: El requisito V2.1.11 no es aplicable para esta aplicación.

CWE relacionado: CWE-521

V2.1.12

Descripción: Verifique que el usuario puede elegir entre ver temporalmente toda la contraseña enmascarada o ver temporalmente el último caracter escrito de la contraseña en plataformas que no tienen esto como funcionalidad integrada.

Estado: NO APLICABLE

Explicación: El requisito V2.1.12 no es aplicable para esta aplicación.

CWE relacionado: CWE-521

V2.2.1

Descripción: Verifique que los controles anti-automatización son efectivos para mitigar las pruebas de credenciales filtradas, fuerza bruta y ataques de bloqueo de cuentas. Estos controles incluyen el bloqueo de las contraseñas filtradas más comunes, bloqueos suaves, limitación de velocidad, CAPTCHA, retrasos cada vez mayores entre intentos, restricciones de direcciones IP o restricciones basadas en riesgos, como la ubicación, el primer inicio de sesión en un dispositivo, los intentos recientes de desbloquear la cuenta o similares. Verifique que no sea posible realizar más de 100 intentos fallidos por hora en una sola cuenta.

Estado: NO APLICABLE

Explicación: El requisito V2.2.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-307

V2.2.2

Descripción: Verifique que el uso de autenticadores débiles (como SMS y correo electrónico) se limita a la verificación secundaria y la aprobación de transacciones y no como un reemplazo para métodos de autenticación más seguros. Verifique que se ofrezcan métodos más fuertes y no métodos débiles, que los usuarios sean conscientes de los riesgos o que se tomen las medidas adecuadas para limitar los riesgos de compromiso de la cuenta.

Estado: NO APLICABLE

Explicación: El requisito V2.2.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-304

V2.2.3

Descripción: Verifique que las notificaciones seguras se envían a los usuarios después de las actualizaciones de los detalles de autenticación, como restablecimientos de credenciales, cambios de correo electrónico o dirección, inicio de sesión desde ubicaciones desconocidas o de riesgo. Se prefiere el uso de notificaciones push - en lugar de SMS o correo electrónico - , pero en ausencia de notificaciones push, SMS o correo electrónico es aceptable siempre y cuando no se divulgue información confidencial en la notificación.

Estado: NO APLICABLE

Explicación: El requisito V2.2.3 no es aplicable para esta aplicación.

CWE relacionado: CWE-620

V2.3.1

Descripción: Verifique que las contraseñas iniciales o los códigos de activación generados por el sistema DEBEN ser generados de forma aleatoreamente segura, DEBE tener al menos 6 caracteres de largo y PUEDE contener letras y números, y expirar después de un corto período de tiempo. Estos secretos iniciales no deben permitirse su re-utilización para convertirse en la contraseña a largo plazo.

Estado: NO APLICABLE

Explicación: El requisito V2.3.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-330

V2.3.2

Descripción: Verifique que se admite la inscripción y el uso de dispositivos de autenticación proporcionados por el suscriptor, como tokens U2F o FIDO.

Estado: NO APLICABLE

Explicación: El requisito V2.3.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-308

V2.3.3

Descripción: Verifique que las instrucciones de renovación se envían con tiempo suficiente para renovar los autenticadores con límite de tiempo.

Estado: NO APLICABLE

Explicación: El requisito V2.3.3 no es aplicable para esta aplicación.

CWE relacionado: CWE-287

V2.4.1

Descripción: Verifique que las contraseñas se almacenan en un forma tal que resisten ataques sin conexión. Las contraseñas DEBERÁN usar hash con salto mediante una derivación de llave de una sola vía aprobada o función de hash de contraseña. Las funciones derivación de llave y hash de contraseñas toman una contraseña, una salto y un factor de costo como entradas al generar un

hash de contraseña. (C6)

Estado: NO APLICABLE

Explicación: El requisito V2.4.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-916

V2.4.2

Descripción: Verifique que el salto tiene al menos 32 bits de longitud y que se elige arbitrariamente para minimizar las colisiones de valor de salto entre los hashes almacenados. Para cada credencial, se DEBE almacenar un único valor de salto y el hash resultante. (C6)

Estado: NO APLICABLE

Explicación: El requisito V2.4.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-916

V2.4.3

Descripción: Verifique que si se utiliza PBKDF2, el recuento de iteraciones DEBE ser tan grande como el rendimiento del servidor de verificación lo permita, normalmente de al menos 100,000 iteraciones. (C6)

Estado: NO APLICABLE

Explicación: El requisito V2.4.3 no es aplicable para esta aplicación.

CWE relacionado: CWE-916

V2.4.4

Descripción: Verifique que si se utiliza bcrypt, el factor de trabajo DEBE ser tan grande como lo permita el rendimiento del servidor de verificación, con un mínimo de 10. (C6)

Estado: NO APLICABLE

Explicación: El requisito V2.4.4 no es aplicable para esta aplicación.

CWE relacionado: CWE-916

V2.4.5

Descripción: Verifique que se realiza una iteración adicional de una función de derivación de claves, utilizando un valor de salto que es secreto y que solo conoce el verificador. Genere el valor de salto utilizando un generador de bits aleatorios aprobado [SP 800-90Ar1] y proporcione al menos la fuerza de seguridad mínima especificada en la última revisión del SP 800-131A. El valor secreto del salto se almacenará por separado de las contraseñas hash (p. ej., en un dispositivo especializado como un módulo de seguridad de hardware).

Estado: NO APLICABLE

Explicación: El requisito V2.4.5 no es aplicable para esta aplicación.

CWE relacionado: CWE-916

V2.5.1

Descripción: Verifique que un secreto de activación o recuperación inicial generado por el sistema no se envíe en texto claro al usuario. (C6)

Estado: NO APLICABLE

Explicación: El requisito V2.5.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-640

V2.5.2

Descripción: Verificar sugerencias de contraseña o autenticación basada en conocimientos (las llamadas "preguntas secretas") no están presentes.

Estado: NO APLICABLE

Explicación: El requisito V2.5.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-640

V2.5.3

Descripción: Verificar la recuperación de credenciales de contraseña no revela la contraseña actual de ninguna manera. (C6)

Estado: NO APLICABLE

Explicación: El requisito V2.5.3 no es aplicable para esta aplicación.

CWE relacionado: CWE-640

V2.5.4

Descripción: Verificar que las cuentas compartidas o predeterminadas no estén presentes (por ejemplo. "root", "admin", o "sa").

Estado: NO APLICABLE

Explicación: El requisito V2.5.4 no es aplicable para esta aplicación.

CWE relacionado: CWE-16

V2.5.5

Descripción: Verifique que si se cambia o reemplaza un factor de autenticación, se notifica al usuario de este evento.

Estado: NO APLICABLE

Explicación: El requisito V2.5.5 no es aplicable para esta aplicación.

CWE relacionado: CWE-304

V2.5.6

Descripción: Verifique la contraseña olvidada y otras rutas de recuperación utilizan un mecanismo de recuperación seguro, como OTP basado en el tiempo (TOTP) u otro token de software, mobile push u otro mecanismo de recuperación sin conexión. (C6)

Estado: NO APLICABLE

Explicación: El requisito V2.5.6 no es aplicable para esta aplicación.

CWE relacionado: CWE-640

V2.5.7

Descripción: Verifique que si se pierden factores de autenticación OTP o multifactor, esa evidencia de prueba de identidad se realiza al mismo nivel que durante la inscripción.

Estado: NO APLICABLE

Explicación: El requisito V2.5.7 no es aplicable para esta aplicación.

CWE relacionado: CWE-308

V2.6.1

Descripción: Verifique que los secretos de búsqueda solo se pueden usar una vez.

Estado: NO APLICABLE

Explicación: El requisito V2.6.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-308

V2.6.2

Descripción: Verifique que los secretos de búsqueda tengan suficiente aleatoriedad (112 bits de entropía), o si menos de 112 bits de entropía, saltados con un única y aleatoria salto de 32 bits y hasheado con un hash aprobado de una sola vía.

Estado: NO APLICABLE

Explicación: El requisito V2.6.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-330

V2.6.3

Descripción: Verifique que los secretos de búsqueda son resistentes a los ataques sin conexión, como los valores predecibles.

Estado: NO APLICABLE

Explicación: El requisito V2.6.3 no es aplicable para esta aplicación.

CWE relacionado: CWE-310

V2.7.1

Descripción: Verifique que los autenticadores de texto sin cifrar fuera de banda tales como PSTN o SMS ("restringido por NIST") no se ofrecen de forma predeterminada, y que en primer lugar se ofrecen alternativas más sólidas, como las notificaciones push.

Estado: NO APLICABLE

Explicación: El requisito V2.7.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-287

V2.7.2

Descripción: Verifique que el verificador fuera de banda expira después de 10 minutos, fuera de las solicitudes de autenticación de banda, códigos o tokens.

Estado: NO APLICABLE

Explicación: El requisito V2.7.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-287

V2.7.3

Descripción: Verifique que las solicitudes de autenticación, los códigos o los tokens de verificador fuera de banda solo se pueden usar una vez y solo para la solicitud de autenticación original.

Estado: NO APLICABLE

Explicación: El requisito V2.7.3 no es aplicable para esta aplicación.

CWE relacionado: CWE-287

V2.7.4

Descripción: Verifique que el autenticador y el verificador fuera de banda se comuniquen a través de un canal independiente seguro.

Estado: NO APLICABLE

Explicación: El requisito V2.7.4 no es aplicable para esta aplicación.

CWE relacionado: CWE-523

V2.7.5

Descripción: Verifique que el verificador fuera de banda conserva solo una versión hasheada del código de autenticación.

Estado: NO APLICABLE

Explicación: El requisito V2.7.5 no es aplicable para esta aplicación.

CWE relacionado: CWE-256

V2.7.6

Descripción: Verifique que el código de autenticación inicial sea generado por un generador de números aleatorios seguro, que contiene al menos 20 bits de entropía (normalmente un número aleatorio digital de seis es suficiente).

Estado: NO APLICABLE

Explicación: El requisito V2.7.6 no es aplicable para esta aplicación.

CWE relacionado: CWE-310

V2.8.1

Descripción: Verifique que los OTP basados en el tiempo tienen una duración definida antes de expirar.

Estado: NO APLICABLE

Explicación: El requisito V2.8.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-613

V2.8.2

Descripción: Verifique que las claves simétricas utilizadas para comprobar los OTP enviados están altamente protegidas, por ejemplo, mediante el uso de un módulo de seguridad de hardware o almacenamiento seguro de claves basadas en el sistema operativo.

Estado: NO APLICABLE

Explicación: El requisito V2.8.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-320

V2.8.3

Descripción: Verifique que los algoritmos criptográficos aprobados se utilizan en la generación, siembra y verificación de OTP.

Estado: NO APLICABLE

Explicación: El requisito V2.8.3 no es aplicable para esta aplicación.

CWE relacionado: CWE-326

V2.8.4

Descripción: Verifique que el OTP basado en el tiempo se pueda utilizar solamente una vez dentro del período de validez.

Estado: NO APLICABLE

Explicación: El requisito V2.8.4 no es aplicable para esta aplicación.

CWE relacionado: CWE-287

V2.8.5

Descripción: Verifique que si se reutiliza un token OTP multifactor basado en el tiempo durante el período de validez, se registra en logs y se rechaza con notificación segura enviada al titular del dispositivo.

Estado: NO APLICABLE

Explicación: El requisito V2.8.5 no es aplicable para esta aplicación.

CWE relacionado: CWE-287

V2.8.6

Descripción: Verifique que el generador OTP de un solo factor físico pueda ser revocado en caso de robo u otra pérdida. Asegúrese de que la revocación es efectiva inmediatamente en todas las sesiones iniciadas, independientemente de la ubicación.

Estado: NO APLICABLE

Explicación: El requisito V2.8.6 no es aplicable para esta aplicación.

CWE relacionado: CWE-613

V2.8.7

Descripción: Verifique que los autenticadores biométricos se limitan a usarlos solo como factores secundarios junto con algo que Ud. tiene y algo que Ud. sabe.

Estado: NO APLICABLE

Explicación: El requisito V2.8.7 no es aplicable para esta aplicación.

CWE relacionado: CWE-308

V2.9.1

Descripción: Verifique que las claves criptográficas utilizadas en la verificación se almacenan de forma segura y protegidas contra la divulgación, como el uso de un módulo de plataforma segura (TPM) o un módulo de seguridad de hardware (HSM) o un servicio de sistema operativo que puede utilizar este almacenamiento seguro.

Estado: NO APLICABLE

Explicación: El requisito V2.9.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-320

V2.9.2

Descripción: Verifique que el mensaje de desafío tenga al menos 64 bits de longitud y sea estadísticamente único o sea único a lo largo de la vida útil del dispositivo criptográfico.

Estado: NO APLICABLE

Explicación: El requisito V2.9.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-330

V2.9.3

Descripción: Verifique que se utilizan algoritmos criptográficos aprobados en la generación, la semilla y la verificación.

Estado: NO APLICABLE

Explicación: El requisito V2.9.3 no es aplicable para esta aplicación.

CWE relacionado: CWE-327

V2.10.1

Descripción: Verifique que los secretos dentro del servicio no se basan en credenciales invariables, como contraseñas, claves de API o cuentas compartidas con acceso con privilegios.

Estado: NO APLICABLE

Explicación: El requisito V2.10.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-287

V2.10.2

Descripción: Verifique que si las contraseñas son necesarias para la autenticación de servicio, la cuenta de servicio utilizada no es una credencial predeterminada. (p. ej., root/root o admin/admin son predeterminados en algunos servicios durante la instalación).

Estado: NO APLICABLE

Explicación: El requisito V2.10.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-255

V2.10.3

Descripción: Verifique que las contraseñas se almacenan con suficiente protección para evitar ataques de recuperación sin conexión, incluido el acceso al sistema local.

Estado: NO APLICABLE

Explicación: El requisito V2.10.3 no es aplicable para esta aplicación.

CWE relacionado: CWE-522

V2.10.4

Descripción: Verifique que las contraseñas, las integraciones con bases de datos y sistemas de terceros, las semillas y los secretos internos y las claves de API se administran de forma segura y no se incluyen en el código fuente ni se almacenan en los repositorios de código fuente. Dicho almacenamiento DEBE resistir ataques fuera de línea. Se recomienda el uso de un almacén de claves de software seguro (L1), TPM de hardware o un HSM (L3) para el almacenamiento de contraseñas.

Estado: NO APLICABLE

Explicación: El requisito V2.10.4 no es aplicable para esta aplicación.

CWE relacionado: CWE-798

Requerimientos ASVS Nivel 2 aplicables:

- No aplicable

Justificación: Aplicación monousuario sin autenticación compleja

V3: Gestión de sesiones

Estado general: NO APLICABLE

Justificación: No utiliza sesiones en el servidor

V3.1.1

Descripción: Verifique que la aplicación nunca revela tokens de sesión en parámetros de dirección URL.

Estado: NO APLICABLE

Explicación: El requisito V3.1.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-598

V3.2.1

Descripción: Verifique que la aplicación genera un nuevo token de sesión en la autenticación de usuario. (C6)

Estado: NO APLICABLE

Explicación: El requisito V3.2.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-384

V3.2.2

Descripción: Verifique que los tokens de sesión posean al menos 64 bits de entropía. (C6)

Estado: NO APLICABLE

Explicación: El requisito V3.2.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-331

V3.2.3

Descripción: Verifique que la aplicación solo almacena tokens de sesión en el navegador mediante métodos seguros, como proteger las cookies adecuadamente (consulte la sección 3.4) o el almacenamiento de sesión en HTML 5.

Estado: NO APLICABLE

Explicación: El requisito V3.2.3 no es aplicable para esta aplicación.

CWE relacionado: CWE-539

V3.2.4

Descripción: Verifique que los tokens de sesión se generan mediante algoritmos criptográficos aprobados. (C6)

Estado: NO APLICABLE

Explicación: El requisito V3.2.4 no es aplicable para esta aplicación.

CWE relacionado: CWE-331

V3.3.1

Descripción: Verifique que el cierre de sesión y la expiración invalidan el token de sesión, de modo que el botón "Atrás" o un usuario de confianza posterior no reanude una sesión autenticada, incluso entre los usuarios de confianza. (C6)

Estado: NO APLICABLE

Explicación: El requisito V3.3.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-613

V3.3.2

Descripción: Si los autenticadores permiten a los usuarios permanecer conectados, compruebe que la re-autenticación se produce periódicamente tanto cuando se utiliza activamente o después de un período de inactividad. (C6)

Estado: NO APLICABLE

Explicación: El requisito V3.3.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-613

V3.3.3

Descripción: Verifique que la aplicación ofrece la opción de terminar todas las demás sesiones activas después de un cambio de contraseña correcto (incluido el cambio mediante el restablecimiento/recuperación de contraseña), y que esto es efectivo en toda la aplicación, el inicio de sesión federado (si está presente) y cualquier usuario de confianza.

Estado: NO APLICABLE

Explicación: El requisito V3.3.3 no es aplicable para esta aplicación.

CWE relacionado: CWE-613

V3.3.4

Descripción: Verifique que los usuarios pueden ver y (habiendo vuelto a introducir las credenciales de inicio de sesión) cerrar sesión en cualquiera o todas las sesiones y dispositivos activos actualmente.

Estado: NO APLICABLE

Explicación: El requisito V3.3.4 no es aplicable para esta aplicación.

CWE relacionado: CWE-613

V3.4.1

Descripción: Verifique que los tokens de sesión basados en cookies tengan el atributo 'Secure' establecido. (C6)

Estado: NO APLICABLE

Explicación: El requisito V3.4.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-614

V3.4.2

Descripción: Verifique que los tokens de sesión basados en cookies tienen el atributo 'HttpOnly' establecido. (C6)

Estado: NO APLICABLE

Explicación: El requisito V3.4.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-1004

V3.4.3

Descripción: Verifique que los tokens de sesión basados en cookies utilizan el atributo 'SameSite' para limitar la exposición a ataques de falsificación de solicitudes entre sitios. (C6)

Estado: NO APLICABLE

Explicación: El requisito V3.4.3 no es aplicable para esta aplicación.

CWE relacionado: CWE-16

V3.4.4

Descripción: Verifique que los tokens de sesión basados en cookies utilizan el prefijo "__Host-" para que las cookies solo se envíen al host que configuró inicialmente la cookie.

Estado: NO APLICABLE

Explicación: El requisito V3.4.4 no es aplicable para esta aplicación.

CWE relacionado: CWE-16

V3.4.5

Descripción: Verifique que si la aplicación se publica bajo un nombre de dominio con otras aplicaciones que establecen o usan cookies de sesión que podrían revelar las cookies de sesión, establezca el atributo de ruta en tokens de sesión basados en cookies utilizando la ruta más precisa posible. (C6)

Estado: NO APLICABLE

Explicación: El requisito V3.4.5 no es aplicable para esta aplicación.

CWE relacionado: CWE-16

V3.5.1

Descripción: Verifique que la aplicación permite a los usuarios revocar tokens de OAuth que forman relaciones de confianza con aplicaciones vinculadas.

Estado: NO APLICABLE

Explicación: El requisito V3.5.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-290

V3.5.2

Descripción: Verifique que la aplicación utiliza tokens de sesión en lugar de claves y secretos de API estáticos, excepto con implementaciones heredadas.

Estado: NO APLICABLE

Explicación: El requisito V3.5.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-798

V3.5.3

Descripción: Verifique que los tokens de sesión sin estado utilizan firmas digitales, cifrado y otras contramedidas para protegerse contra ataques de manipulación, envolvente, reproducción, cifrado nulo y sustitución de claves.

Estado: NO APLICABLE

Explicación: El requisito V3.5.3 no es aplicable para esta aplicación.

CWE relacionado: CWE-345

V3.7.1

Descripción: Verifique que la aplicación garantiza una sesión de inicio de sesión completa y válida o requiere una re-autenticación o verificación secundaria antes de permitir cualquier transacción confidencial o modificaciones de la cuenta.

Estado: NO APLICABLE

Explicación: El requisito V3.7.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-306

Requerimientos ASVS Nivel 2 aplicables:

- No aplicable

Justificación: No utiliza sesiones en el servidor

V4: Control de Acceso

Estado general: NO APLICABLE

Justificación: Aplicación monousuario sin control de acceso entre usuarios

V4.1.1

Descripción: Verifique que la aplicación aplica las reglas de control de acceso en una capa de servicio de confianza, especialmente si el control de acceso del lado cliente está presente y podría ser bypaseado.

Estado: NO APLICABLE

Explicación: El requisito V4.1.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-602

V4.1.2

Descripción: Verifique que todos los atributos de usuario y datos y la información de directiva utilizada por los controles de acceso no pueden ser manipulados por los usuarios finales a menos que se autorice específicamente.

Estado: NO APLICABLE

Explicación: El requisito V4.1.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-639

V4.1.3

Descripción: Verifique que existe el principio de privilegios mínimos: los usuarios solo deben poder acceder a funciones, archivos de datos, direcciones URL, controladores, servicios y otros recursos, para los que poseen una autorización específica. Esto implica protección contra la suplantación y elevación de privilegios. (C7)

Estado: NO APLICABLE

Explicación: El requisito V4.1.3 no es aplicable para esta aplicación.

CWE relacionado: CWE-285

V4.1.5

Descripción: Verifique que los controles de acceso fallan de forma segura, incluso cuando se produce una excepción. (C10)

Estado: NO APLICABLE

Explicación: El requisito V4.1.5 no es aplicable para esta aplicación.

CWE relacionado: CWE-285

V4.2.1

Descripción: Verifique que los datos confidenciales y las API están protegidos contra ataques de referencia insegura directa de objetos (IDOR; por sus siglas en inglés) dirigidos a la creación, lectura, actualización y eliminación de registros, como la creación o actualización del registro de otra persona, la visualización de los registros de todos o la eliminación de todos los registros.

Estado: NO APLICABLE

Explicación: El requisito V4.2.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-639

V4.2.2

Descripción: Verifique que la aplicación o el framework aplica un mecanismo anti-CSRF seguro para proteger la funcionalidad autenticada, y eficaz anti-automatización o anti-CSRF protege la funcionalidad no autenticada.

Estado: NO APLICABLE

Explicación: El requisito V4.2.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-352

V4.3.1

Descripción: Verifique que las interfaces administrativas utilicen la autenticación multifactor adecuada para evitar el uso no autorizado.

Estado: NO APLICABLE

Explicación: El requisito V4.3.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-419

V4.3.2

Descripción: Verifique que la exploración de directorios está deshabilitada a menos que se desee deliberadamente. Además, las aplicaciones no deben permitir la detección o divulgación de metadatos de archivos o directorios, como Thumbs.db, .DS_Store, .git o .svn.

Estado: NO APLICABLE

Explicación: El requisito V4.3.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-548

V4.3.3

Descripción: Verifique que la aplicación tiene autorización adicional (como la autenticación paso a paso o adaptativa) para sistemas de menor valor y/ o segregación de tareas para aplicaciones de alto valor para aplicar controles antifraude según el riesgo de aplicación y fraudes previos.

Estado: NO APLICABLE

Explicación: El requisito V4.3.3 no es aplicable para esta aplicación.

CWE relacionado: CWE-732

Requerimientos ASVS Nivel 2 aplicables:

- No aplicable

Justificación: Aplicación monousuario sin control de acceso entre usuarios

V5: Validación, Desinfección y Codificación

V5.1.1

Descripción: Verifique que la aplicación tiene defensas contra los ataques de contaminación de parámetros HTTP, especialmente si el marco de la aplicación no hace ninguna distinción sobre el origen de los parámetros de solicitud (GET, POST, cookies, encabezados o variables de entorno).

Estado: PARCIAL

Explicación: El requisito V5.1.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-235

V5.1.2

Descripción: Verifique que los frameworks protegen contra ataques de asignación de parámetros masivos o que la aplicación tiene contramedidas para proteger contra la asignación de parámetros no seguros, como marcar campos privados o similares. (C5)

Estado: PARCIAL

Explicación: El requisito V5.1.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-915

V5.1.3

Descripción: Verifique que todas las entradas (campos de formulario HTML, solicitudes REST, parámetros de URL, encabezados HTTP, cookies, archivos por lotes, fuentes RSS, etc.) se validan mediante validación positiva (lista de permitidos). (C5)

Estado: PARCIAL

Explicación: El requisito V5.1.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-20

V5.1.4

Descripción: Verifique que las estructuras de datos están fuertemente tipados y validados con un esquema definido que incluya caracteres permitidos, longitud y patrón (p. ej., números de tarjeta de

crédito, direcciones de correo electrónico, números de teléfono, o validar que dos campos relacionados son razonables, como comprobar que el suburbio y el código postal coinciden). (C5)

Estado: PARCIAL

Explicación: El requisito V5.1.4 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-20

V5.1.5

Descripción: Verifique que las redirecciones y reenvíos de URL solo permiten destinos que aparecen en una lista de permitidos, o muestra una advertencia al redirigir a contenido potencialmente no confiable.

Estado: PARCIAL

Explicación: El requisito V5.1.5 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-601

V5.2.1

Descripción: Verifique que todas las entradas HTML que no son de confianza de los editores WYSIWYG o similares se sanitizan correctamente con una biblioteca de sanitización HTML o una función de marco de trabajo. (C5)

Estado: PARCIAL

Explicación: El requisito V5.2.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-116

V5.2.2

Descripción: Verifique que los datos no estructurados están sanitizados para aplicar medidas de seguridad, como caracteres permitidos y longitud.

Estado: PARCIAL

Explicación: El requisito V5.2.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-138

V5.2.3

Descripción: Verifique que la aplicación sanitiza la entrada del usuario antes de pasar a los sistemas de correo para protegerse contra la inyección SMTP o IMAP.

Estado: PARCIAL

Explicación: El requisito V5.2.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-147

V5.2.4

Descripción: Verifique que la aplicación evita el uso de eval() u otras características de ejecución de código dinámico. Cuando no hay alternativa, cualquier entrada de usuario debe sanitizarse, y ponerlo en sandbox antes de ejecutarse.

Estado: PARCIAL

Explicación: El requisito V5.2.4 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-95

V5.2.5

Descripción: Verifique que la aplicación protege contra ataques de inyección de plantilla asegurándose que cualquier entrada de usuario que se incluya está sanitizada o en un lugar controlado.

Estado: PARCIAL

Explicación: El requisito V5.2.5 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-94

V5.2.6

Descripción: Verifique que la aplicación protege contra ataques SSRF, validando o desinfectando datos que no son de confianza o metadatos de archivos HTTP, como nombres de archivo y campos de entrada de URL, y utiliza listas de protocolos permitidos, dominios, rutas de acceso y puertos.

Estado: PARCIAL

Explicación: El requisito V5.2.6 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-918

V5.2.7

Descripción: Verifique que la aplicación desinfecta, deshabilita o pone en sandbox el contenido proporcionado por el usuario, con scripts de gráficos vectoriales escalables (SVG; por sus siglas en inglés) especialmente en lo que se refiere a XSS resultante de scripts en línea y foreignObject.

Estado: PARCIAL

Explicación: El requisito V5.2.7 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-159

V5.2.8

Descripción: Verifique que la aplicación desinfecta, deshabilita o pone en sandbox el contenido proporcionado por el usuario, con expresiones en lenguaje de plantilla o script como Markdown, CSS o las hojas de estilo XSL, BBCode o similares.

Estado: PARCIAL

Explicación: El requisito V5.2.8 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-94

V5.3.1

Descripción: Verifique que la codificación de salida es relevante para el intérprete y el contexto requerido. Por ejemplo, utilice codificadores específicamente para valores HTML, atributos HTML, JavaScript, parámetros de URL, encabezados HTTP, SMTP y otros según lo requiera el contexto, especialmente a partir de entradas que no sean de confianza (por ejemplo, nombres con Unicode o apóstrofes, como u O'Hara). (C4)

Estado: PARCIAL

Explicación: El requisito V5.3.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-116

V5.3.2

Descripción: Verifique que la codificación de salida conserva el juego de caracteres y la configuración regional elegidos por el usuario, de modo que cualquier punto de caracteres Unicode sea válido y se maneje de forma segura. (C4)

Estado: PARCIAL

Explicación: El requisito V5.3.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-176

V5.3.3

Descripción: Verifique que el escape de salida basado en contexto, preferiblemente automatizado - o en el peor de los casos, manual - protege contra XSS reflejado, almacenado y basado en DOM. (C4)

Estado: PARCIAL

Explicación: El requisito V5.3.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-79

V5.3.4

Descripción: Verifique que la selección de datos o las consultas de base de datos (por ejemplo, SQL, HQL, ORM, NoSQL) utilizan consultas parametrizadas, ORM, marcos de entidades o están protegidas de los ataques de inyección de base de datos. (C3)

Estado: PARCIAL

Explicación: El requisito V5.3.4 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-89

V5.3.5

Descripción: Verifique donde los mecanismos parametrizados o más seguros no están presentes, la codificación de la salida en el contexto específico se utiliza para proteger contra ataques de inyección, como el uso de escape SQL para proteger contra la inyección SQL. (C3, C4)

Estado: PARCIAL

Explicación: El requisito V5.3.5 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-89

V5.3.6

Descripción: Verifique que la aplicación protege contra ataques de inyección de JSON, ataques de "eval" en JSON y evaluación de expresiones de JavaScript. (C4)

Estado: PARCIAL

Explicación: El requisito V5.3.6 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-830

V5.3.7

Descripción: Verifique que la aplicación protege contra vulnerabilidades de inyección LDAP o que se han implementado controles de seguridad específicos para evitar la inyección LDAP. (C4)

Estado: PARCIAL

Explicación: El requisito V5.3.7 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-90

V5.3.8

Descripción: Verifique que la aplicación protege contra la inyección de comandos del sistema operativo y que las llamadas al sistema operativo utilizan consultas de sistema operativo parametrizadas o utilicen codificación de salida de línea de comandos contextual. (C4)

Estado: PARCIAL

Explicación: El requisito V5.3.8 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-78

V5.3.9

Descripción: Verifique que la aplicación protege contra ataques de inclusión de archivos locales (LFI) o de inclusión remota de archivos (RFI).

Estado: PARCIAL

Explicación: El requisito V5.3.9 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-829

V5.3.10

Descripción: Verifique que la aplicación protege contra ataques de inyección XPath o de inyección XML. (C4)

Estado: PARCIAL

Explicación: El requisito V5.3.10 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-643

V5.4.1

Descripción: Verifique que la aplicación utiliza cadenas de memoria segura, copia de memoria más segura y aritmética de puntero para detectar o evitar desbordamientos de pila, búffer o heap.

Estado: CUMPLE

Explicación: El requisito V5.4.1 se cumple según el análisis realizado.

CWE relacionado: CWE-120

V5.4.2

Descripción: Verifique que las cadenas de formato no toman entradas potencialmente hostiles y son constantes.

Estado: CUMPLE

Explicación: El requisito V5.4.2 se cumple según el análisis realizado.

CWE relacionado: CWE-134

V5.4.3

Descripción: Verifique que se utilizan técnicas de validación de signos, intervalos y entradas para evitar desbordamientos de enteros.

Estado: CUMPLE

Explicación: El requisito V5.4.3 se cumple según el análisis realizado.

CWE relacionado: CWE-190

V5.5.1

Descripción: Verifique que los objetos serializados utilizan comprobaciones de integridad o están cifrados para evitar la creación de objetos hostiles o la manipulación de datos. (C5)

Estado: PARCIAL

Explicación: El requisito V5.5.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-502

V5.5.2

Descripción: Verifique que la aplicación restringe correctamente los analizadores XML para que solo usen la configuración más restrictiva posible y para asegurarse de que las características no seguras, como la resolución de entidades externas, están deshabilitadas para evitar ataques XML eXternal Entity (XXE).

Estado: PARCIAL

Explicación: El requisito V5.5.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-611

V5.5.3

Descripción: Verifique que la deserialización de datos que no son de confianza se evita o está protegida tanto en código personalizado como en bibliotecas de terceros (como analizadores JSON, XML y YAML).

Estado: PARCIAL

Explicación: El requisito V5.5.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-502

V5.5.4

Descripción: Verifique que al analizar JSON en exploradores o backends basados en JavaScript, JSON.parse se utiliza para analizar el documento JSON. No utilice eval() para analizar JSON.

Estado: PARCIAL

Explicación: El requisito V5.5.4 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-95

Estado de cumplimiento: PARCIAL

Explicación detallada:

V5.1: Falta validación en alguna de las capas (frontend o backend). Se recomienda implementar validación en ambas capas para defensa en profundidad.

V6: Criptografía almacenada

Estado general: NO APLICABLE

Justificación: Datos almacenados localmente en cliente, no en servidor

V6.1.1

Descripción: Verifique que los datos privados regulados se almacenan cifrados mientras están en reposo, como información de identificación personal (PII), información personal confidencial o datos evaluados que puedan estar sujetos al RGPD de la UE.

Estado: NO APLICABLE

Explicación: El requisito V6.1.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-311

V6.1.2

Descripción: Verifique que los datos de salud regulados se almacenen cifrados mientras están en reposo, como registros médicos, detalles de dispositivos médicos o registros de investigación anonimizados.

Estado: NO APLICABLE

Explicación: El requisito V6.1.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-311

V6.1.3

Descripción: Verifique que los datos financieros regulados se almacenen cifrados mientras están en reposo, como cuentas financieras, impagos o historial de crédito, registros fiscales, historial de pagos, beneficiarios o registros de mercado o de investigación anonimizados.

Estado: NO APLICABLE

Explicación: El requisito V6.1.3 no es aplicable para esta aplicación.

CWE relacionado: CWE-311

V6.2.1

Descripción: Verifique que todos los módulos criptográficos fallan de forma segura y que los errores se gestionan de forma que no se habiliten los ataques "Padding Oracle".

Estado: NO APLICABLE

Explicación: El requisito V6.2.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-310

V6.2.2

Descripción: Verifique que se utilicen algoritmos, modos y bibliotecas criptográficas probados por la industria o aprobados por el gobierno, en lugar de criptografía codificada personalizada. (C8)

Estado: NO APLICABLE

Explicación: El requisito V6.2.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-327

V6.2.3

Descripción: Verifique que los modos de vector de inicialización de cifrado, configuración de cifrado y bloque están configurados de forma segura mediante los últimos consejos vigentes.

Estado: NO APLICABLE

Explicación: El requisito V6.2.3 no es aplicable para esta aplicación.

CWE relacionado: CWE-326

V6.2.4

Descripción: Verifique que los algoritmos de número aleatorio, cifrado o hash, longitudes de clave, rondas, cifrados o modos, se puedan reconfigurar, actualizar o intercambiar en cualquier momento, para protegerse contra ruptura criptográficas. (C8)

Estado: NO APLICABLE

Explicación: El requisito V6.2.4 no es aplicable para esta aplicación.

CWE relacionado: CWE-326

V6.2.5

Descripción: Verifique que los modos de bloque inseguros conocidos (i.e., ECB, etc.), los modos de relleno (i.e. PKCS#1 v1.5, etc.), los cifrados con tamaños de bloque pequeños (i.e. Triple-DES, Blowfish, etc.), y los algoritmos de hashing débiles (i.e. MD5, SHA1, etc.) no se utilizan a menos que sea necesario para la compatibilidad con versiones anteriores.

Estado: NO APLICABLE

Explicación: El requisito V6.2.5 no es aplicable para esta aplicación.

CWE relacionado: CWE-326

V6.2.6

Descripción: Verifique que los "nonces", los vectores de inicialización y otros números de uso único no se deben usar más de una vez con una clave de cifrado determinada. El método de generación debe ser adecuado para el algoritmo que se está utilizando.

Estado: NO APLICABLE

Explicación: El requisito V6.2.6 no es aplicable para esta aplicación.

CWE relacionado: CWE-326

V6.3.1

Descripción: Verifique que todos los números aleatorios, nombres de archivo aleatorios, GUID aleatorios y cadenas aleatorias se generan utilizando el generador de números aleatorios criptográficamente seguro aprobado por el módulo criptográfico cuando estos valores aleatorios están destinados a no ser adivinables por un atacante.

Estado: NO APLICABLE

Explicación: El requisito V6.3.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-338

V6.3.2

Descripción: Verifique que los GUID aleatorios se crean mediante el algoritmo GUID v4 y un generador de números pseudoaleatorio (CSPRNG) criptográficamente seguro. Los GUID creados con otros generadores de números pseudoaleatorios pueden ser predecibles.

Estado: NO APLICABLE

Explicación: El requisito V6.3.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-338

V6.4.1

Descripción: Verifique que una solución de gestión de secretos, como un almacén de claves, se utiliza para crear, almacenar, controlar el acceso y destruir secretos de forma segura. (C8)

Estado: NO APLICABLE

Explicación: El requisito V6.4.1 no es aplicable para esta aplicación.

CWE relacionado: CWE-798

V6.4.2

Descripción: Verifique que el material de claves no está expuesto a la aplicación, sino que utiliza un módulo de seguridad aislado como un almacén para operaciones criptográficas. (C8)

Estado: NO APLICABLE

Explicación: El requisito V6.4.2 no es aplicable para esta aplicación.

CWE relacionado: CWE-320

Requerimientos ASVS Nivel 2 aplicables:

- No aplicable

Justificación: Datos almacenados localmente en cliente, no en servidor

V7: Manejo y Registro de Errores

V7.1.1

Descripción: Verifique que la aplicación no registra las credenciales ni los detalles de pago. Los tokens de sesión solo deben almacenarse en registros de forma irreversible y hasheados. (C9, C10)

Estado: PARCIAL

Explicación: El requisito V7.1.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-532

V7.1.2

Descripción: Verifique que la aplicación no registra otros datos confidenciales tal como se definen en las leyes de privacidad locales o la política de seguridad pertinente. (C9)

Estado: PARCIAL

Explicación: El requisito V7.1.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-532

V7.1.3

Descripción: Verifique que la aplicación registra eventos relevantes para la seguridad, incluidos los eventos de autenticación correctos y con errores, los errores de control de acceso, los errores de deserialización y los errores de validación de entrada. (C5, C7)

Estado: PARCIAL

Explicación: El requisito V7.1.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-778

V7.1.4

Descripción: Verifique que cada evento de registro incluye la información necesaria que permitiría una investigación detallada de la escala de tiempo cuando se produce un evento. (C9)

Estado: PARCIAL

Explicación: El requisito V7.1.4 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-778

V7.2.1

Descripción: Verifique que se registran todas las decisiones de autenticación, sin almacenar tokens o contraseñas de sesión confidenciales. Esto debe incluir solicitudes con los metadatos relevantes necesarios para las investigaciones de seguridad.

Estado: PARCIAL

Explicación: El requisito V7.2.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-778

V7.2.2

Descripción: Verifique que se pueden registrar todas las decisiones de control de acceso y que se registran todas las decisiones erróneas. Esto debe incluir solicitudes con los metadatos pertinentes necesarios para las investigaciones de seguridad.

Estado: PARCIAL

Explicación: El requisito V7.2.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-285

V7.3.1

Descripción: Verifique que todos los componentes de registro codifiquen adecuadamente los datos para evitar la inyección de registros. (C9)

Estado: PARCIAL

Explicación: El requisito V7.3.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-117

V7.3.3

Descripción: Verifique que los registros de seguridad están protegidos contra el acceso y la modificación no autorizados. (C9)

Estado: PARCIAL

Explicación: El requisito V7.3.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-200

V7.3.4

Descripción: Verifique que la fuente donde se lee el tiempo están sincronizados con la hora y la zona horaria correctas. Considere firmemente el registro solo en UTC si los sistemas son globales para ayudar con el análisis forense posterior al incidente. (C9)

Estado: PARCIAL

Explicación: El requisito V7.3.4 se cumple parcialmente. Se requiere revisión adicional.

V7.4.1

Descripción: Verifique que se muestra un mensaje genérico cuando se produce un error inesperado o sensible a la seguridad, potencialmente con un identificador único que el personal de soporte técnico puede usar para investigar. (C10)

Estado: PARCIAL

Explicación: El requisito V7.4.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-210

V7.4.2

Descripción: Verifique que el control de excepciones (o un equivalente funcional) se utiliza en todo el código base para tener en cuenta las condiciones de error esperadas e inesperadas. (C10)

Estado: PARCIAL

Explicación: El requisito V7.4.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-544

V7.4.3

Descripción: Verifique que se define un controlador de errores de "último recurso" que detectará todas las excepciones no controladas. (C10)

Estado: PARCIAL

Explicación: El requisito V7.4.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-431

Estado de cumplimiento: PARCIAL

Explicación detallada:

V7.1: Falta implementación estructurada de manejo de errores

V8: Protección de Datos

V8.1.1

Descripción: Verifique que la aplicación protege los datos confidenciales de la caché en componentes del servidor, como balanceadores de carga y cachés de aplicaciones.

Estado: PARCIAL

Explicación: El requisito V8.1.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-524

V8.1.2

Descripción: Verifique que todas las copias almacenadas en caché o temporales de datos confidenciales almacenados en el servidor están protegidas contra el acceso no autorizado o purgadas/invalidadas después de que el usuario autorizado acceda a los datos confidenciales.

Estado: PARCIAL

Explicación: El requisito V8.1.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-524

V8.1.3

Descripción: Verifique que la aplicación minimiza el número de parámetros de una solicitud, como campos ocultos, variables Ajax, cookies y valores de encabezado.

Estado: PARCIAL

Explicación: El requisito V8.1.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-233

V8.1.4

Descripción: Verifique que la aplicación puede detectar y alertar sobre números anormales de solicitudes, como por IP, usuario, total por hora o día, o lo que tenga sentido para la aplicación.

Estado: PARCIAL

Explicación: El requisito V8.1.4 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-770

V8.2.1

Descripción: Verifique que la aplicación establece suficientes encabezados anti-almacenamiento en caché para que los datos confidenciales no se almacenen en caché en los navegadores modernos.

Estado: PARCIAL

Explicación: El requisito V8.2.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-525

V8.2.2

Descripción: Verifique que los datos almacenados en el almacenamiento del navegador (como localStorage, sessionStorage, IndexedDB o cookies) no contengan datos confidenciales.

Estado: PARCIAL

Explicación: El requisito V8.2.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-922

V8.2.3

Descripción: Verifique que los datos autenticados se borran del almacenamiento del cliente, como el DOM del explorador, después de que se termine el cliente o la sesión.

Estado: PARCIAL

Explicación: El requisito V8.2.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-922

V8.3.1

Descripción: Verifique que los datos confidenciales se envían al servidor en el cuerpo o encabezados del mensaje HTTP y que los parámetros de cadena de consulta de cualquier verbo HTTP no contienen datos confidenciales.

Estado: PARCIAL

Explicación: El requisito V8.3.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-319

V8.3.2

Descripción: Verifique que los usuarios tienen un método para eliminar o exportar sus datos sobre demanda (on demand).

Estado: PARCIAL

Explicación: El requisito V8.3.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-212

V8.3.3

Descripción: Verifique que se proporciona a los usuarios un lenguaje claro con respecto a la recopilación y el uso de la información personal suministrada y que los usuarios han proporcionado el consentimiento de aceptación para el uso de esos datos antes de que se utilicen de alguna manera.

Estado: PARCIAL

Explicación: El requisito V8.3.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-285

V8.3.4

Descripción: Verifique que se han identificado todos los datos confidenciales creados y procesados por la aplicación, y asegúrese de que existe una política sobre cómo tratar los datos confidenciales. (C8)

Estado: PARCIAL

Explicación: El requisito V8.3.4 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-200

V8.3.5

Descripción: Verifique que el acceso a los datos confidenciales se audita (sin registrar los datos confidenciales en sí), si los datos se recopilan en las directivas de protección de datos pertinentes o donde se requiere el registro del acceso.

Estado: PARCIAL

Explicación: El requisito V8.3.5 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-532

V8.3.6

Descripción: Verifique que la información confidencial contenida en la memoria se sobrescribe tan pronto como ya no sea necesaria para mitigar los ataques de volcado de memoria, utilizando ceros o datos aleatorios.

Estado: PARCIAL

Explicación: El requisito V8.3.6 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-226

V8.3.7

Descripción: Verifique que la información confidencial o privada que se requiere que se cifre, se cifra mediante algoritmos aprobados que proporcionan confidencialidad e integridad. (C8)

Estado: PARCIAL

Explicación: El requisito V8.3.7 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-327

V8.3.8

Descripción: Verifique que la información personal confidencial está sujeta a la clasificación de retención de datos, de forma que los datos antiguos o desactualizados se eliminen automáticamente, según una programación o según la situación lo requiera.

Estado: PARCIAL

Explicación: El requisito V8.3.8 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-285

Estado de cumplimiento: PARCIAL

Explicación detallada:

V8.1: Las validaciones defensivas están implementadas pero podrían ser más exhaustivas en todas las operaciones críticas

V9: Comunicación

V9.1.1

Descripción: Verifique que TLS se utilice para toda la conectividad del cliente y que no recurra a comunicaciones inseguras o no cifradas. (C8)

Estado: PARCIAL

Explicación: El requisito V9.1.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-319

V9.1.2

Descripción: Verifique con herramientas de prueba TLS actualizadas que solo estén habilitados los conjuntos de cifrado fuertes, con los conjuntos de cifrado más fuertes configurados como preferidos.

Estado: PARCIAL

Explicación: El requisito V9.1.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-326

V9.1.3

Descripción: Verifique que solo estén habilitadas las últimas versiones recomendadas del protocolo TLS, como TLS 1.2 y TLS 1.3. La última versión del protocolo TLS debería ser la opción preferida.

Estado: PARCIAL

Explicación: El requisito V9.1.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-326

V9.2.1

Descripción: Verifique que las conexiones hacia y desde el servidor utilizan certificados TLS de confianza. Cuando se utilizan certificados generados internamente o autofirmados, el servidor debe configurarse para que solo confíe en las CA internas específicas y en los certificados autofirmados específicos. Todos los demás deben ser rechazados.

Estado: PARCIAL

Explicación: El requisito V9.2.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-295

V9.2.2

Descripción: Verifique que las comunicaciones cifradas, como TLS, se utilizan para todas las conexiones entrantes y salientes, incluidos los puertos de administración, monitoreo, la autenticación, la API o las llamadas a servicios web, la base de datos, la nube, el serverless, el mainframe, ya sean externos o de conexiones de asociados. El servidor no debe volver a protocolos inseguros o no cifrados.

Estado: PARCIAL

Explicación: El requisito V9.2.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-319

V9.2.3

Descripción: Verifique que se autentican todas las conexiones cifradas a sistemas externos que implican información o funciones confidenciales.

Estado: PARCIAL

Explicación: El requisito V9.2.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-287

V9.2.4

Descripción: Verifique que la adecuada revocación de certificación, como la comprobación de Online Certificate Status Protocol (OCSP), esté habilitada y configurada.

Estado: PARCIAL

Explicación: El requisito V9.2.4 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-299

Estado de cumplimiento: PARCIAL

Explicación detallada:

V9.1: La aplicación actualmente utiliza HTTP. Se recomienda HTTPS para producción para proteger las comunicaciones.

V10: Código Malicioso

V10.2.1

Descripción: Verifique que el código fuente de la aplicación y las bibliotecas de terceros no contienen capacidades no autorizadas de recopilación de datos o de "llamadas a casa". Cuando detecte dicha funcionalidad, obtenga el permiso explicito del usuario para que sea operado así, antes de recopilar cualquier dato.

Estado: PARCIAL

Explicación: El requisito V10.2.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-359

V10.2.2

Descripción: Verifique que la aplicación no solicite permisos innecesarios o excesivos para funciones o sensores relacionados con la privacidad, como contactos, cámaras, micrófonos o ubicación.

Estado: PARCIAL

Explicación: El requisito V10.2.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-272

V10.3.1

Descripción: Verifique si la aplicación tiene una característica de actualización automática de cliente o servidor, las actualizaciones deben obtenerse a través de canales seguros y firmados digitalmente. El código de actualización debe validar la firma digital de la actualización antes de instalar o ejecutar la actualización.

Estado: PARCIAL

Explicación: El requisito V10.3.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-16

V10.3.2

Descripción: Verifique que la aplicación emplea protecciones de integridad, como la firma de código o la integridad de subrecursos. La aplicación no debe cargar ni ejecutar código de fuentes que no sean de confianza, como la carga de includes, plugins, módulos, código o bibliotecas de fuentes que no sean de confianza o de Internet.

Estado: PARCIAL

Explicación: El requisito V10.3.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-353

V10.3.3

Descripción: Verifique que la aplicación tiene protección contra takeovers de subdominios si la aplicación se basa en entradas DNS o subdominios DNS, como nombres de dominio expirados, punteros DNS obsoletos o CNAME, proyectos expirados en repositorios de código fuente públicos o API de nube transitorias, funciones serverless o buckets de almacenamiento (autogen-bucket-id.cloud.example.com) o similares. Las protecciones pueden incluir asegurarse de que los nombres DNS utilizados por las aplicaciones se comprueban regularmente para comprobar su caducidad o cambio.

Estado: PARCIAL

Explicación: El requisito V10.3.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-350

Estado de cumplimiento: PARCIAL

Explicación detallada:

V10.1: La validación de entrada podría ser más exhaustiva

V11: Lógica de Negocio

V11.1.1

Descripción: Verificar que la aplicación solo procesará flujos de la lógica de negocio para el mismo usuario en orden de pasos secuenciales y sin omitir pasos.

Estado: PARCIAL

Explicación: El requisito V11.1.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-841

V11.1.2

Descripción: Verificar que la aplicación solo procesará flujos de lógica de negocios con todos los pasos que se procesan en tiempo humano realista, es decir, las transacciones no se envían demasiado rápido.

Estado: PARCIAL

Explicación: El requisito V11.1.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-799

V11.1.3

Descripción: Verificar que la aplicación tiene límites adecuados para acciones o transacciones de negocio específicas, y que se aplican correctamente con base en los usuarios.

Estado: PARCIAL

Explicación: El requisito V11.1.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-770

V11.1.4

Descripción: Verifique que la aplicación tenga controles anti-automatización para proteger contra llamadas excesivas, como exfiltración masiva de datos, solicitudes de lógica empresarial, carga de archivos o ataques de denegación de servicio.

Estado: PARCIAL

Explicación: El requisito V11.1.4 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-770

V11.1.5

Descripción: Verificar que la aplicación tiene límites de lógica empresarial o validación para protegerse contra riesgos o amenazas empresariales probables, identificados mediante el modelado de amenazas o metodologías similares.

Estado: PARCIAL

Explicación: El requisito V11.1.5 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-841

V11.1.6

Descripción: Verifique que la aplicación no tenga problemas de "Time Of Check to Time Of Use" (TOCTOU) u otras race conditions para operaciones sensibles.

Estado: PARCIAL

Explicación: El requisito V11.1.6 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-367

V11.1.7

Descripción: Verificar que la aplicación supervisa eventos o actividades inusuales desde una perspectiva de lógica de negocios. Por ejemplo, los intentos de realizar acciones fuera de servicio o acciones que un usuario normal nunca intentaría. (C9)

Estado: PARCIAL

Explicación: El requisito V11.1.7 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-754

V11.1.8

Descripción: Verificar que la aplicación tiene alertas configurables cuando se detectan ataques automatizados o actividad inusual.

Estado: PARCIAL

Explicación: El requisito V11.1.8 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-390

Estado de cumplimiento: PARCIAL

Explicación detallada:

V11.1: La lógica de negocio podría estar mejor centralizada

V12: Archivos y Recursos

V12.1.1

Descripción: Verifique que la aplicación no aceptará archivos grandes que puedan llenar el almacenamiento o provocar una denegación de servicio.

Estado: PARCIAL

Explicación: El requisito V12.1.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-400

V12.1.2

Descripción: Verifique que la aplicación compruebe los archivos comprimidos (p. ej. zip, gz, docx, odt) contra el tamaño máximo sin comprimir permitido y con el número máximo de archivos antes de descomprimir el archivo.

Estado: PARCIAL

Explicación: El requisito V12.1.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-409

V12.1.3

Descripción: Verifique que se aplica una cuota de tamaño de archivo y un número máximo de archivos por usuario para asegurarse de que un solo usuario no puede llenar el almacenamiento con demasiados archivos o archivos excesivamente grandes.

Estado: PARCIAL

Explicación: El requisito V12.1.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-770

V12.2.1

Descripción: Verifique que los archivos obtenidos de orígenes que no son de confianza se validan para que sean del tipo esperado en función del contenido del archivo.

Estado: PARCIAL

Explicación: El requisito V12.2.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-434

V12.3.1

Descripción: Verifique que los metadatos del nombre de archivo enviados por el usuario no se utilizan directamente por los sistemas de archivos del sistema o del marco de trabajo y que se utiliza una API de dirección URL para proteger contra el recorrido de ruta de acceso.

Estado: PARCIAL

Explicación: El requisito V12.3.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-22

V12.3.2

Descripción: Verifique que los metadatos del nombre de archivo enviados por el usuario se validan o ignoran para evitar la divulgación, creación, actualización o eliminación de archivos locales (LFI).

Estado: PARCIAL

Explicación: El requisito V12.3.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-73

V12.3.3

Descripción: Verifique que los metadatos del nombre de archivo enviados por el usuario se validan o omiten para evitar la divulgación o ejecución de archivos remotos a través de ataques de inclusión remota de archivos (RFI) o falsificación de solicitudes del lado del servidor (SSRF).

Estado: PARCIAL

Explicación: El requisito V12.3.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-98

V12.3.4

Descripción: Verifique que la aplicación protege contra la descarga de archivos reflectantes (RFD) validando o ignorando los nombres de archivo enviados por el usuario en un parámetro JSON, JSONP o URL, el encabezado Content-Type de respuesta debe establecerse en text/plain y el encabezado Content-Disposition debe tener un nombre de archivo fijo.

Estado: PARCIAL

Explicación: El requisito V12.3.4 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-641

V12.3.5

Descripción: Verifique que los metadatos de archivos que no son de confianza no se utilizan directamente con la API del sistema o las bibliotecas, para proteger contra la inyección de comandos del sistema operativo.

Estado: PARCIAL

Explicación: El requisito V12.3.5 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-78

V12.3.6

Descripción: Verifique que la aplicación no incluye ni ejecuta funcionalidad desde orígenes que no son de confianza, como redes de distribución de contenido no verificadas, bibliotecas de JavaScript, bibliotecas node npm o archivos DLL server-side.

Estado: PARCIAL

Explicación: El requisito V12.3.6 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-829

V12.4.1

Descripción: Verifique que los archivos obtenidos de fuentes no confiables se almacenen fuera de la raíz web, con permisos limitados.

Estado: PARCIAL

Explicación: El requisito V12.4.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-552

V12.4.2

Descripción: Verifique que los escáneres antivirus analicen los archivos obtenidos de fuentes no confiables para evitar la carga y el servicio de contenido malicioso conocido.

Estado: PARCIAL

Explicación: El requisito V12.4.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-509

V12.5.1

Descripción: Verifique que la capa web está configurado para transmitir solo archivos con extensiones específicas, para evitar la filtración accidental de información o código fuente. Por ejemplo, los archivos de copia de seguridad (p. ej. .bak), los archivos de trabajo temporales (p. ej. .swp), los archivos comprimidos (.zip, .tar.gz, etc.) y otras extensiones utilizadas comúnmente por los editores deben bloquearse a menos que sea necesario.

Estado: PARCIAL

Explicación: El requisito V12.5.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-552

V12.5.2

Descripción: Verifique que las solicitudes directas a los archivos cargados nunca se ejecutarán como contenido HTML/JavaScript.

Estado: PARCIAL

Explicación: El requisito V12.5.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-434

V12.6.1

Descripción: Verifique que el servidor web o de aplicaciones está configurado con una lista de permisos de recursos o sistemas a los que el servidor puede enviar solicitudes o cargar datos o archivos.

Estado: PARCIAL

Explicación: El requisito V12.6.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-918

Estado de cumplimiento: PARCIAL

Explicación detallada:

V12.1: Parcialmente aplicable - Solo los endpoints de importación/exportación de DefectDojo manejan archivos

V13: API y Servicios Web

V13.1.1

Descripción: Verifique que todos los componentes de la aplicación utilizan las mismas codificaciones y analizadores para evitar el análisis de ataques que explotan un comportamiento de análisis de archivos o URI diferente que se podría usar en ataques SSRF y RFI.

Estado: PARCIAL

Explicación: El requisito V13.1.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-116

V13.1.3

Descripción: Verifique que las direcciones URL de la API no exponen información confidencial, como API keys, los tokens de sesión, etc.

Estado: PARCIAL

Explicación: El requisito V13.1.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-598

V13.1.4

Descripción: Verifique que las decisiones de autorización se toman en el URI, se aplican mediante seguridad programática o declarativa en el controlador o enrutador, y en el nivel de recursos, se aplican mediante permisos basados en modelos.

Estado: PARCIAL

Explicación: El requisito V13.1.4 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-285

V13.1.5

Descripción: Verifique que las solicitudes que contienen tipos de contenido inesperados o contenido que falta se rechazan con encabezados adecuados (estado de respuesta HTTP 406 Inaceptable o 415 Tipo de medio no compatible).

Estado: PARCIAL

Explicación: El requisito V13.1.5 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-434

V13.2.1

Descripción: Verifique que los métodos HTTP RESTful habilitados son una opción válida para el usuario o la acción, como impedir que los usuarios normales usen DELETE o PUT en recursos o API protegidos.

Estado: PARCIAL

Explicación: El requisito V13.2.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-650

V13.2.2

Descripción: Verifique que la validación del esquema JSON está en su lugar y se comprueba antes de aceptar la entrada.

Estado: PARCIAL

Explicación: El requisito V13.2.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-20

V13.2.3

Descripción: Verifique que los servicios web RESTful que utilizan cookies están protegidos contra la falsificación de solicitudes entre sitios, mediante el uso de una o más de las siguientes formas: patrón de cookies de doble envío, "nonces" CSRF o comprobaciones de encabezado de solicitud de origen.

Estado: PARCIAL

Explicación: El requisito V13.2.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-352

V13.2.5

Descripción: Verifique que los servicios REST comprueben explícitamente que el tipo de contenido entrante sea el esperado, como application/xml o application/json.

Estado: PARCIAL

Explicación: El requisito V13.2.5 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-436

V13.2.6

Descripción: Verifique que los encabezados de mensaje y la carga útil (payload) son confiables y no se modifican en tránsito. Requerir un cifrado seguro para el transporte (solo TLS) puede ser suficiente en muchos casos, ya que proporciona confidencialidad y protección de integridad. Las firmas digitales por cada mensaje pueden proporcionar una garantía adicional sobre las protecciones de transporte para aplicaciones de alta seguridad, pero conllevan complejidad y riesgos adicionales para compensar los beneficios.

Estado: PARCIAL

Explicación: El requisito V13.2.6 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-345

V13.3.1

Descripción: Verifique que la validación del esquema XSD tiene lugar para garantizar un documento XML formado correctamente, seguido de la validación de cada campo de entrada antes de que se realice cualquier procesamiento de esos datos.

Estado: PARCIAL

Explicación: El requisito V13.3.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-20

V13.3.2

Descripción: Verifique que el payload del mensaje está firmada mediante WS-Security para garantizar un transporte fiable entre el cliente y el servicio.

Estado: PARCIAL

Explicación: El requisito V13.3.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-345

V13.4.1

Descripción: Verifique que se utiliza una lista de permisos de consulta o una combinación de limitación de profundidad y limitación de cantidad para evitar que GraphQL o la expresión de la capa de datos provoque una denegación de servicio (DoS) como resultado de costosas consultas anidadas. Para escenarios más avanzados, se debe usar el análisis de costos de consulta.

Estado: PARCIAL

Explicación: El requisito V13.4.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-770

V13.4.2

Descripción: Verifique que GraphQL u otra lógica de autorización de capa de datos podría implementarse en la capa de lógica de negocio en lugar de la capa GraphQL.

Estado: PARCIAL

Explicación: El requisito V13.4.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-285

Estado de cumplimiento: PARCIAL

Explicación detallada:

V13.1: La documentación de la API podría mejorarse

V14: Configuración

V14.1.1

Descripción: Verifique que los procesos de compilación y despliegue de aplicaciones se realizan de forma segura y repetible, como la automatización de CI/CD, la administración de configuración automatizada y los scripts de despliegue automatizado.

Estado: PARCIAL

Explicación: El requisito V14.1.1 se cumple parcialmente. Se requiere revisión adicional.

V14.1.2

Descripción: Verifique que los indicadores del compilador están configurados para habilitar todas las protecciones y advertencias de desbordamiento de búfer disponibles, incluida la aleatorización de la pila, la prevención de la ejecución de datos y para interrumpir la compilación si se encuentra un puntero no seguro, memoria, cadena de formato, entero u operaciones de cadena.

Estado: PARCIAL

Explicación: El requisito V14.1.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-120

V14.1.3

Descripción: Verifique que la configuración del servidor está hardenizada según las recomendaciones del servidor de aplicaciones y los framewors en uso.

Estado: PARCIAL

Explicación: El requisito V14.1.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-16

V14.1.4

Descripción: Verifique que la aplicación, la configuración y todas las dependencias se pueden volver a implementar mediante scripts de implementación automatizada, crearse a partir de un runbook documentado y probado en un tiempo razonable o restaurarse a partir de copias de seguridad de forma oportuna.

Estado: PARCIAL

Explicación: El requisito V14.1.4 se cumple parcialmente. Se requiere revisión adicional.

V14.2.1

Descripción: Verifique que todos los componentes estén actualizados, preferiblemente utilizando un comprobador de dependencias durante el tiempo de compilación. (C2)

Estado: PARCIAL

Explicación: El requisito V14.2.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-1026

V14.2.2

Descripción: Verifique que se eliminen todas las funciones, documentación, aplicaciones de muestra y configuraciones innecesarias.

Estado: PARCIAL

Explicación: El requisito V14.2.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-1002

V14.2.3

Descripción: Verifique que si los activos de la aplicación, como bibliotecas JavaScript, fuentes CSS o web, se hospedan externamente en una red de entrega de contenido (CDN) o un proveedor

externo, se usa la integridad de subrecursos (SRI) para validar la integridad del activo.

Estado: PARCIAL

Explicación: El requisito V14.2.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-829

V14.2.4

Descripción: Verifique que los componentes de terceros provienen de repositorios predefinidos, de confianza y mantenidos continuamente. (C2)

Estado: PARCIAL

Explicación: El requisito V14.2.4 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-829

V14.2.5

Descripción: Verifique que se mantenga una Lista de materiales de software (SBOM; por sus siglas en inglés) de todas las bibliotecas de terceros en uso. (C2)

Estado: PARCIAL

Explicación: El requisito V14.2.5 se cumple parcialmente. Se requiere revisión adicional.

V14.2.6

Descripción: Verifique que la superficie de ataque se reduce mediante sandboxing o encapsular bibliotecas de terceros para exponer solo el comportamiento necesario en la aplicación. (C2)

Estado: PARCIAL

Explicación: El requisito V14.2.6 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-265

V14.3.2

Descripción: Verifique que los modos de depuración del servidor web o de aplicaciones y del framework de aplicaciones están deshabilitados en producción para eliminar las características de depuración, las consolas de desarrollador y las divulgaciones de seguridad no deseadas.

Estado: PARCIAL

Explicación: El requisito V14.3.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-497

V14.3.3

Descripción: Verifique que los encabezados HTTP o cualquier parte de la respuesta HTTP no exponen información detallada de la versión de los componentes del sistema.

Estado: PARCIAL

Explicación: El requisito V14.3.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-200

V14.4.1

Descripción: Verifique que cada respuesta HTTP contenga un encabezado de tipo de contenido. También especifique un conjunto de caracteres seguro (p. ej., UTF-8, ISO-8859-1) si los tipos de contenido son texto/*, /+xml y aplicación/xml. El contenido debe coincidir con el encabezado de tipo de contenido proporcionado.

Estado: PARCIAL

Explicación: El requisito V14.4.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-173

V14.4.2

Descripción: Verifique que todas las respuestas de API contienen un encabezado Content-Disposition: attachment; filename="api.json" (u otro nombre de archivo apropiado para el tipo de contenido).

Estado: PARCIAL

Explicación: El requisito V14.4.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-116

V14.4.3

Descripción: Verifique que existe un encabezado de respuesta de Directiva de Seguridad de Contenido (CSP) que ayuda a mitigar el impacto de los ataques XSS como vulnerabilidades de inyección de HTML, DOM, JSON y JavaScript.

Estado: PARCIAL

Explicación: El requisito V14.4.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-1021

V14.4.4

Descripción: Verifique que todas las respuestas contienen un encabezado X-Content-Type-Options: nosniff.

Estado: PARCIAL

Explicación: El requisito V14.4.4 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-116

V14.4.5

Descripción: Verifique que se incluye un encabezado Strict-Transport-Security en todas las respuestas y para todos los subdominios, como Strict-Transport-Security: max-age-15724800; includeSubdomains.

Estado: PARCIAL

Explicación: El requisito V14.4.5 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-523

V14.4.6

Descripción: Verifique que se incluya adecuadamente un encabezado de Referrer-Policy para evitar exponer información confidencial en la URL a través del encabezado de referencia a partes que no son de confianza.

Estado: PARCIAL

Explicación: El requisito V14.4.6 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-116

V14.4.7

Descripción: Verifique que el contenido de una aplicación web no se puede incrustar en un sitio de terceros de forma predeterminada y que la inserción de los recursos exactos solo se permite cuando sea necesario mediante el uso adecuado de Content-Security-Polic: frame-ancestors y encabezados de respuesta X-Frame-Options.

Estado: PARCIAL

Explicación: El requisito V14.4.7 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-1021

V14.5.1

Descripción: Verifique que el servidor de aplicaciones solo acepta los métodos HTTP que utiliza la aplicación/API, incluidas las pre-flight OPTIONS, y los Logs/alertas en cualquier solicitud que no sea válida para el contexto de la aplicación.

Estado: PARCIAL

Explicación: El requisito V14.5.1 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-749

V14.5.2

Descripción: Verifique que el encabezado Origin proporcionado no se utiliza para las decisiones de autenticación o control de acceso, ya que un atacante puede cambiar fácilmente el encabezado Origin.

Estado: PARCIAL

Explicación: El requisito V14.5.2 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-346

V14.5.3

Descripción: Verifique que el encabezado Cross-Origin Resource Sharing (CORS) Access-Control-Allow-Origin utiliza una estricta lista de permisos de dominios y subdominios de confianza para que coincidan entre si, y no se permita el origen "nulo".

Estado: PARCIAL

Explicación: El requisito V14.5.3 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-346

V14.5.4

Descripción: Verifique que la aplicación autentica los encabezados HTTP agregados por un proxy de confianza o dispositivos SSO, como un token de portador.

Estado: PARCIAL

Explicación: El requisito V14.5.4 se cumple parcialmente. Se requiere revisión adicional.

CWE relacionado: CWE-306

Estado de cumplimiento: PARCIAL

Explicación detallada:

V14.1: La configuración podría estar mejor centralizada

5. Análisis WSTG (OWASP Web Security Testing Guide)

5.1. Introducción al WSTG

El OWASP Web Security Testing Guide (WSTG) es una guía completa para probar la seguridad de aplicaciones web y servicios web. Proporciona un marco de mejores prácticas utilizado por profesionales de seguridad y organizaciones en todo el mundo.

Este análisis se basa en los findings de WSTG almacenados en DefectDojo, obtenidos mediante la sincronización bidireccional con el WSTG Tracker.

5.2. Resumen de Tests WSTG

Total de tests WSTG analizados: 3

Distribución por estado:

- In Progress: 3

5.3. Tests WSTG por Categoría

5.3.INFO. INFO: Information Gathering

Tests encontrados: 2

• WSTG-INFO-01: WSTG-INFO-01: Conduct OSINT Reconnaissance
• Estado: In Progress
• Severidad: Info
• WSTG-INFO-02: WSTG-INFO-02: Fingerprint Web Server
• Estado: In Progress
• Severidad: Info

5.4. Detalles de Tests WSTG

A continuación se detallan los tests WSTG más relevantes:

5.4.1. WSTG-AUTHN-01: WSTG-AUTHN-01: Test Credentials

• Estado: In Progress
• Severidad: Medium
• Descripción: WSTG test: Test Credentials

5.4.2. WSTG-INFO-01: WSTG-INFO-01: Conduct OSINT Reconnaissance

• Estado: In Progress
• Severidad: Info
• Descripción: WSTG test: Conduct OSINT reconnaissance

5.4.3. WSTG-INFO-02: WSTG-INFO-02: Fingerprint Web Server

• Estado: In Progress
• Severidad: Info
• Descripción: WSTG test: Fingerprint Web Server

6. Recomendaciones y Próximos Pasos

6.1. Resumen del Estado Actual

La aplicación implementa buenas prácticas de seguridad en validación de entrada, headers de seguridad y manejo defensivo de datos.

6.2. Mejoras Recomendadas

Para alcanzar el cumplimiento completo del ASVS Nivel 2, se recomienda implementar las siguientes mejoras:

• Validación de tipos numéricos: Implementar validación explícita de NaN e Infinity
• CORS en producción: Restringir CORS a orígenes específicos en producción
• Logging mejorado: Implementar logging estructurado de errores

7. Referencias

• OWASP ASVS (página principal)

- OWASP ASVS 4.0.3 en GitHub (versión utilizada en este informe)
- OWASP ASVS 4.0.3 - Categorías de verificación
- OWASP ASVS 5.0 (versión actual)
- OWASP WSTG (Web Security Testing Guide)